Anno XXII - N°2 (196) • Periodicità: bimestrale • Marzo/Aprile 2020 • 10/02/2020
RIVISTA+DVD DOUBLE SIDE € 8,99

DVD DOPPIO

MARZO/APRILE 2020

EDIZIONI MASTER
www.edmaster.it

00196
9 771592 815006

MACCHINE VIRTUALI VS CONTAINER

VIRTUALIZZAZZIONE COSA ASPETTI?

Con la nostra guida pratica scegli (e implementi subito) la soluzione giusta per ogni evenienza

GRATIS SUL DVD ESEMPI PRONTI ALL'USO

WI-FI SOTTO ATTACCO

Scopri i punti deboli delle reti wireless, come identificarli con una scansione, e cosa fare per arginare il pericolo

DIGITAL HOME

UN REGISTRATORE DI CASSA FOSS

Una soluzione economica e altamente personalizzabile per tutti i commercianti

GAMING

THE MAGIC CIRCLE

Un gioco apparentemente incompleto, ma ricco di humour nero

RETE CISCO CCNA

- Configuriamo l'accesso SSH a uno switch
- Attiviamo le porte dal terminale

SISTEMA

DA WINDOWS 7 A KUBUNTU

Terminato il supporto a Windows 7 è giunto il momento di passare a Linux!

HARDWARE

IL TUO NUOVO NOTEBOOK LOWCOST!

Economici sì, lenti no: ecco i migliori device per ufficio, coding... e non solo

Poste Italiane S.p.A. - Spedizione in abbonamento postale - D.L. 353/2003 (conv. in L. 27/02/2004 n.46) art. 1, comma 1, Aut. GIPA/S/CS/12/2011 • Distributore esclusivo: Distribuzione SO.DI.P. "Angelo Patuzzi" S.p.A., Via Bettola n. 18, 20092 Cinisello Balsamo (MI)

LINUX Magazine

Anno XXII - 2 (196) - Marzo/Aprile 2020
Periodicità bimestrale - 10/02/2020
Reg. Trib. di CS n.ro 625 del 23 Febbraio 1999
Codice ISSN 1592- 8152

Direttore Responsabile: Massimo Mattone
Responsabile Editoriale: Gianmarco Bruni

Collaboratore redazionale: Luca Tringali
Collaboratori: M. Petrecca

Progetto grafico e Art Director: Paolo Cristiano
Grafica: Fabiola Grandinetti, Beppe Salvagnoni

Concessionaria per la pubblicità: MEDIAADV S.r.l.
Via Antonio Panizzi, 6, 20146 Milano
Tel. 02.43986531
e-mail: info@mediaadv.it

EDITORE Edizioni Master S.p.A.
Via Bartolomeo Diaz, 13 - 87036 Rende (CS)

Presidente e Amministratore Delegato: Massimo Sesti

ARRETRATI
Costo arretrati (a copia): il doppio del prezzo di copertina + € 6,10 (spedizione con corriere).
Per informazioni e richieste, inviare un'e-mail all'indirizzo arretrati@edmaster.it

Assistenza tecnica: linuxmagazine@edmaster.it

SERVIZIO CLIENTI
servizioclienti@edmaster.it

Stampa: Arti Grafiche Boccia S.p.A.
Via T. C. Felice, 7 - 84131 Salerno
Duplicazione DVD: DUPLAS AVELCA srl
Via G.P. Clerici, 11 - 21040 Gerenzano (VA)

Distributore esclusivo per l'Italia:
Distribuzione SO.DI.P. "Angelo Patuzzi" S.p.A., Via Bettola n. 18, 20092 Cinisello Balsamo (MI), Tel. 02.660301 - 02.66030320

Finito di stampare: Febbraio 2020

"Rispettare l'uomo e l'ambiente in cui esso vive e lavora è una parte di tutto ciò che facciamo e di ogni decisione che prendiamo per assicurare che le nostre operazioni siano basate sul continuo miglioramento delle performance ambientali e sulla prevenzione dell'inquinamento"

LINUX Magazine n. 196

Editoriale

Conoscenza è libertà

Se non si conosce il funzionamento di una tecnologia, non si può essere davvero liberi di utilizzarla. Naturalmente non si può immaginare che tutti abbiano una conoscenza approfondita di ogni argomento, ma nella società dell'informazione è fondamentale avere almeno una idea di massima di come funzionino le tecnologie a cui ci affidiamo. È bene sapere quando possiamo stare tranquilli e quando, invece, dobbiamo insospettirci. Per questo motivo spieghiamo nella cover story la differenza tra macchine virtuali e container: si tratta di due tecnologie molto utilizzate per implementare le varie applicazioni web che usiamo ogni giorno, ma che offrono un livello di sicurezza molto diverso, ed è importante sapere che non sono del tutto interscambiabili. Ed è per lo stesso motivo che continuiamo il nostro corso di Penetration Testing presentando la falla della crittografia Wi-Fi WPA2: a causa dell'attacco KRACK le informazioni che inviamo al nostro router possono essere intercettate. Sempre per questo motivo continuiamo a invogliare gli utenti, anche i meno esperti, a provare GNU/Linux. Nessun sistema può garantire protezione assoluta, ma è un dato di fatto indiscutibile che GNU/Linux sia più sicuro di Windows. Per questo proponiamo un tutorial passo passo per installare Kubuntu sul proprio PC. E ne offriamo anche una versione con l'interfaccia simile a Windows nel DVD allegato alla Linux Magazine, per aiutare chi non ha mai usato GNU/Linux. Perché, quando ci si rivolge a un potenziale nuovo utente, dire "passa a Linux" non basta: bisogna anche impegnarsi per rendere la transizione indolore.

Luca Tringali
Invia il tuo commento a:
linuxmagazine@edmaster.it

Seguici anche su *http://bit.ly/linuxmagazine* *http://bit.ly/redditlinuxmag* *http://bit.ly/facelinuxmag*

MACCHINE VIRTUALI VS CONTAINER

docker

GRATIS SUL DVD ESEMPI PRONTI ALL'USO

Con la nostra guida pratica scegli (e implementi subito) la soluzione giusta per ogni evenienza *pag. 10*

DVD DOPPIO LATO A

Distribuzioni

ANITA OS 18.04

PER CHI PASSA DA WINDOWS A LINUX

Con l'uscita di scena di Windows 7, molti utenti non sono convinti di voler passare a Windows 10. È un sistema troppo invasivo della privacy degli utenti, e si porta appresso le varie problematiche tipiche di Windows. Alcuni utenti potrebbero quindi essere interessati a passare a GNU/Linux, ma è chiaro che per un principiante possa non essere facile abituarsi subito a un nuovo sistema operativo. Considerando che la maggioranza delle persone fa affidamento all'aspetto grafico, riconoscendo immediatamente le icone e la disposizione degli elementi sul desktop, abbiamo realizzato una versione modificata di Kubuntu che offre un ambiente grafico configurato per assomigliare il più possibile proprio a Windows. Questo per rendere più agevole la transizione al nuovo sistema operativo, mantenendo almeno l'aspetto simile a quanto si è abituati a vedere da anni. Sul sistema sono anche preinstallati tutti i principali programmi necessari per gli uffici pubblici, le aziende, le scuole, e l'utilizzo domestico.

DVD DOPPIO LATO B

Tools

LA WEB APP DI COWSAY

VM E CONTAINER A CONFRONTO

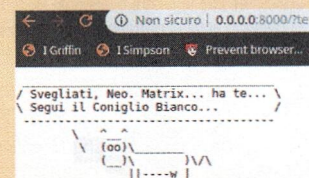
Nel lato B del DVD presentiamo una web app realizzata con poche righe di codice in Python, che si limita a prendere un testo e farlo apparire in ascii art con l'output del famoso comando cowsay. La web app è distribuita sia in un container Docker che in un disco per VirtualBox, così da poterli provare e toccare con mano le differenze tra macchine virtuali e container. Il file cowsay.tar è l'immagine per il container Docker. Per importarla nel poprrio Docker basta il comando

```
sudo docker load --in
        put cowsay.tar
```

si può poi eseguire così:

```
sudo docker run --rm -it
      -p 8000:8000 cowsay
```

l'interfaccia web si troverà al proprio indirizzo IP locale, solitamente 0.0.0.0, porta 8000.

Il file cowsay.vdi è invece l'immagine disco virtuale di una macchina virtuale VirtualBox. Conviene creare una macchina virtuale di tipo Linux 64bit e scheda di rete con bridge. Poi si può specificare come disco il file vdi e avviare la macchina. La password dell'utente root è "root".

C'è il BookMagazine giusto **per ogni tua passione!**

Qual è il software Linux giusto per proteggere i documenti? Come ottimizzare il sistema? Ecco le soluzioni ai problemi comuni e le dritte per usare al top la distro Ubuntu.

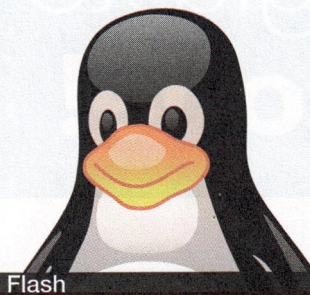
Una guida completa, un vero e proprio ABC di WhatsApp, che ti svela tutti i segreti di questa celebre app di messaggistica e ti offre anche molti utili consigli pratici.

Ciò che si può realizzare con Excel può supportare ogni tipo di attività. Questo libro è indispensabile per chi vuole arricchire il curriculum vitae e trovare lavoro nel mondo hi-tech.

Al giorno d'oggi chi ha a che fare in qualche modo con la comunicazione non può fare a meno di avere un proprio sito Web o un blog. Questo è il libro che ti consentirà di debuttare su Internet da vero protagonista!

Servizi, programmi, impostazioni e le giuste dritte per proteggersi sul Web impedendo a siti malevoli, pirati informatici e truffatori di rintracciare la tua identità

I nostri esperti ti spiegano passo dopo passo come utilizzare le funzioni nascoste del sistema operativo made in Redmond per sfruttare al massimo PC, Internet e app come non hai mai fatto prima.

Flash

KDE: lo strumento per il feedback

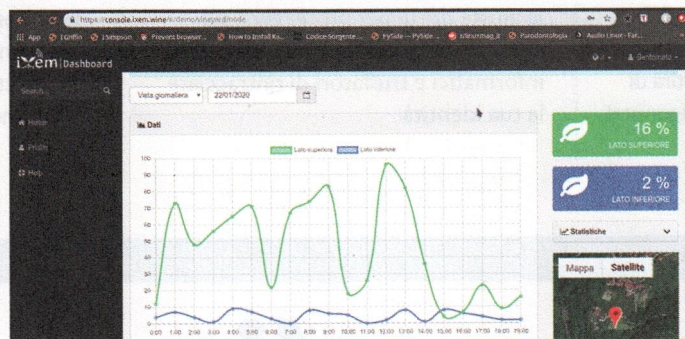
Il nuovo KDE Plasma avrà un'app che permetterà agli utenti l'invio di feedback sui vari software. Al momento KDE dispone infatti di un sistema per la segnalazione dei bug, ma è un meccanismo scomodo per gli utenti e viene utilizzato quasi soltanto da sviluppatori. Questo causa un circolo vizioso, perché gli sviluppatori finiscono per parlare solo con se stessi, e vedere solo il proprio punto di vista. Col nuovo strumento User Feedback sarà possibile indicare cosa non funziona e quali siano i propri gusti senza installare strumenti di debug.
Fonte: *http://bit.ly/prolilearningaou*

Wine 5.0 è arrivato

Gli sviluppatori di Wine hanno rilasciato la versione 5.0. Le novità si concentrano molto sull'aspetto grafico, che è stato il suo tasto dolente. È stato migliorato il supporto a Vulkan e alle DirectX, in modo da poter visualizzare interfacce grafiche che fanno uso di effetti 3D, trasparenze, ecc. Si spera che questo faciliti l'uso di software tutt'ora molto richiesti, come la suite Adobe. Questo va unito al fatto che le varie librerie sono compilati nel formato PE, quello degli eseguibili Windows. Questo rende molto più semplice l'interazione tra i programmi degli utenti e il software Wine, velocizzando l'esecuzione e riducendo l'incompatibilità. Purtroppo è ancora presente una versione piuttosto vecchia. Per fortuna sul sito Wine sono disponibili istruzioni per tutte le principali distribuzioni, per aggiungere dei repository che contengono le ultime versioni di Wine.
Fonte: *http://bit.ly/nuovowine50*

Una connessione wireless a 700 km di distanza

Il Politecnico di Torino ha presentato una tecnologia di trasmissione dati via radio che ha funzionato con una distanza di oltre 700km tra trasmettitore e ricevitore: è il futuro dell'Internet a basso costo

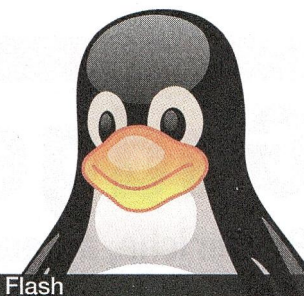
Solitamente si parla dell'IoT in termini domestici: un frigorifero intelligente, una centralina domotica con riconoscimento vocale, un cardiofrequenzimetro che si collega allo smartphone e ci avvisa in caso di aritmia. Ma la realtà è che questi sono solo "giocattoli", utili per vivere in modo più semplice e forse più ecologico. L'Internet of Things diventerà davvero importante, invece, soprattutto nell'automazione sul lavoro. Soprattutto nel settore primario, agricoltura e allevamento, è ormai chiaro che i tradizionali metodi produttivi basati in gran parte sul lavoro umano non sono più sostenibili, se non per una minima produzione di lusso. Con l'aumento della popolazione e la maggiore richiesta di cibo a basso costo sarà necessario implementare sistemi di gestione di piantagioni e allevamenti automatici e dotati di sensori, che possano quindi sfruttare le teorie agronomiche per rendere la produzione più efficiente, meno dannosa per il territorio, e meno costosa per il consumatore. Dobbiamo quindi immaginare grandi campi di coltivazioni e bestiame non sorvegliati dall'uomo: a gestire ogni aspetto, soprattutto la protezione da eventi meteorologici, saranno sensori e computer. L'uomo non sarà mai completamente esterno alla gestione di queste fattorie futuristiche, ma si troverà a molti chilometri di distanza, dentro una università o comunque qualche ufficio, monitorando da lontano le informazioni che provengono dai sensori e il funzionamento dei meccanismi robotizzati. Questo però apre un problema: buona parte delle coltivazioni e degli allevamenti saranno sempre situati in luoghi lontani dalle grandi città, ed è probabile che non sarà mai economicamente vantaggioso portare in quei luoghi un collegamento internet con una banda sufficiente a garantire il controllo remoto delle apparecchiature 24 ore su 24. In effetti, soprattutto in un paese come l'Italia, la principale sfida per l'Internet of Things è proprio la prima parola: Internet. La connettività rimarrà un problema, perché tirare cavi tra Alpi e Appennini è molto costoso. L'unica soluzione è procedere con sistemi senza fili, ma devono essere a lunga distanza: anche il classico WiMax, che offre una distanza massima di 10Km, non è sufficiente perché implica che bisognerebbe comunque portare la linea via cavo ogni decina di chilometri, e rischia di essere comunque troppo costoso. Il Politecnico di Torino sta però lavorando su una soluzione per la connettività a basso costo, già da molti anni. E di recente è riuscito a ottenere una **connessione wireless** alla distanza record di **700 km.** Il laboratorio iXem del Politecnico ha sviluppato molti sensori nel corso degli anni ma l'ultimo prototipo presentato, chiamato iXemWine, sembra davvero il coronamento del lavoro svolto per abbattere il digital divide. Questi sensori sono stati progettati, come suggerisce il nome, per misurare vari parametri agro-meteorologici nelle vigne e rendere più efficienti i trattamenti fitosanitari, necessari per produrre un buon vino. Per realizzare il test in condizioni reali e con il minore costo possibile, i ricercatori dell'iXem Lab hanno alimentato i loro sensori con due semplici pile stilo alcaline, e realizzato le antenne per la trasmissione del dati con dei semplici palloni aerostatici ancorati al terreno, invece di costruire costosi e ingombranti tralicci. Il sensore con trasmettitore radio è stato posizionato in **Sardegna**, nelle vigne di Carloforte, e il suo segnale è stato ricevuto ogni 10 minuti addirittura da un ricevitore installato a Tarragona, in **Catalogna** (Spagna), a una distanza di oltre 700km. Questo grazie a un sistema di trasmissione talmente ottimizzato da richiedere pochissima energia anche per la trasmissione su enormi distanze: dopo sei mesi di trasmissioni continue, la carica delle due pile stilo è diminuita appena del 10%. "Oggi", ha dichiarato il Direttore di iXem Labs Daniele Trinchero, "sperimentiamo dispositivi compatti, di facile installazione, a bassissime emissioni, con fabbisogno energetico minimo, e quindi replicabili. Questa sarà l'Internet del futuro".

AnBox Cloud: eseguire applicazioni Android in cloud

Molti servizi utili alla vita quotidiana sono disponibili solo come app Android. Perché non eseguirli da qualsiasi dispositivo grazie al cloud di Canonical

Ormai ci stiamo abituando ai servizi in streaming: non si tratta più soltanto musica e film, ma anche applicazioni. Google Stadia ha infatti dimostrato che può avere senso offrire un servizio di streaming per videogiocatori: ogni utente può giocare da casa, ma l'app viene eseguita sul cloud Google e avviene semplicemente un trasferimento di dati riguardante l'interfaccia grafica e i comandi dell'utente. Questo rende possibile accedere ai videogame da qualsiasi dispositivo, senza bisogno di rincorrere continuamente l'ultimo modello di scheda grafica. Seguendo la stessa filosofia, Canonical ha sviluppato AnBox Cloud: un sistema basato su container per virtualizzare applicazioni Android su un desktop Linux. L'idea è semplice: visto che ormai molte applicazioni importanti e soprattutto bisognose di risorse sono rilasciate come app Android, si può offrire un servizio che permetta agli utenti di eseguire qualsiasi tipo di app da qualunque dispositivo. Il vero obiettivo a cui punta Canonical è la realtà virtuale: con l'arrivo del 5G sarà teoricamente possibile lavorare a distanza. Pensiamo alla chirurgia mininvasiva da remoto in tempo reale, il controllo di robot aziendali, la gestione di sistemi di sicurezza per gli edifici. In caso di una operazione difficile, un chirurgo molto esperto potrà lavorare anche in ospedali periferici con guanti e visore connessi al PC dell'ufficio, mentre una applicazione eseguita sui server ARM potrà interpretare i movimenti e trasmetterli ai robot chirurgici. Al momento è possibile richiedere un test della tecnologia, ma solo se si è operatori di telefonia. Canonical per adesso non prevede di offrire il servizio direttamente agli utenti.

NextCloud Hub: l'alternativa libera alle Google Apps

Sincronizzazione, suite office, email, videochiamate: tutto dal proprio browser col software libero

Un'azienda o una pubblica amministrazione hanno spesso bisogno di un ambiente collaborativo per permettere ai propri dipendenti di condividere documenti, scambiare email, lavorare contemporaneamente e comunicare in modo diretto. La soluzione tipica è l'utilizzo di Google Apps For Business. Il problema di affidarsi ai servizi Big G è che il suo modello si business si basa in buona parte, sul controllo dei file o dei metadati in modo da propinarci pubblicità mirata. Inoltre, i file risiedendo su server Google, non possiamo essere certi che siano sempre accessibili. Per dati sensibili può essere una buona idea gestire tutto internamente, e il nuovo Nextcloud Hub si propone di fare proprio questo: è un ambiente completo che non offre solo la sincronizzazione e una interfaccia web per accedere ai propri file, ma anche gallerie fotografiche, una suite office web collaborativa, un calendario, un'interfaccia le email e una web app per videochiamate tra colleghi. Si tratta della soluzione perfetta per ogni ufficio e è tutta open source. Per uffici piccoli NextCloud può essere installato su un semplice server "casalingo" (*http://bit.ly/nextclouddevice*) come gli UBOSbox, che costano meno di 300 euro e hanno un disco da 120GB, oppure il Nextcloud Home/SME server, che costa 850 euro ma offre un disco da 2TB e ben 16GB di RAM. È ovviamente anche possibile installare il pacchetto NextCloud Hub su un proprio server virtuale.

Flash

Linux in un biglietto da visita

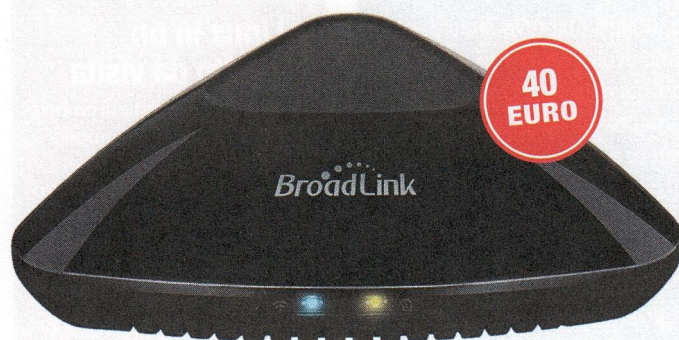
Un ingegnere di sistemi embedded ha realizzato, nel proprio tempo libero, un minuscolo computer che può stare dentro un biglietto da visita, e che è in grado di funzionare tramite Linux. Si tratta più che altro di un esercizio, ma dimostra quanto il sistema operativo GNU/Linux sia versatile: il dispositivo è solo leggermente più spesso di un comune biglietto da visita, ha la stessa superficie, e dispone di una porta USB per collegarsi al terminale. Esegue il boot in circa 6 secondi, e presenta il curriculum vitae più una serie di fotografie dell'ingegnere. Chi è interessato a replicare la cosa può leggere codice sorgente e istruzioni sul repository GitHub ufficiale del progetto BusinessCardLinux.
Fonte: *http://bit.ly/businesscardlinux*

Firefox 72 migliora la sicurezza

Firefox si è sempre proposto come il browser perfetto per chi è preoccupato dalla propria privacy. La nuova release, la numero 72, punta molto sempre nella stessa direzione. Innanzitutto, vengono disabilitati automaticamente vari sistemi di tracciamento, che alcuni siti usano per riconoscere gli utenti al di là dei cookie. Vengono anche nascoste per opzione predefinita le fastidiose notifiche dei siti. Inoltre, è disponibile anche una funzionalità molto comoda per gli utenit: il Picture in Picture. In poche parole, se si sta guardando un video (da YouTube o altri siti) è possibile farlo apparire in un piccolo popup sullo schermo mentre ci si sposta su altre schede.
Fonte: *http://bit.ly/firefox72*

I BEST BUY DEL MESE

Gadget hi-tech per tutti

Periferiche, accessori e altri dispositivi per lavorare e divertirsi nel tempo libero

IL TELECOMANDO UNIVERSALE

BROADLINK RM PRO+

Grazie a questo dispositivo possiamo dire addio a tutti i telecomandi che ci ritroviamo sul divano: quello della TV, quello del decoder, del condizionatore e dell'home theater. Grazie all'app ufficiale, infatti, potremo prima memorizzare tutte le frequenze e dopo comandare qualsiasi dispositivo IR o RF presente nei paraggi maneggiando unicamente il nostro smartphone.

Per informazioni: ***http://bit.ly/2Enwfor***

SUPER IPCAM IN ULTRAHD

ARLO ULTRA

Di IP Cam ce ne sono a bizzeffe. Ma questa soluzione di Arlo (spin-off di Netgear) è un vero e proprio sistema di sicurezza unico nel suo genere: le telecamere sono infatti completamente wireless. Non necessitano neppure di un cavo di alimentazione, poiché alimentate da delle batterie che offrono un'autonomia di diversi mesi. La cam (il kit è espandibile con tutte le telecamere di cui necessitiamo) è impermeabile e resistente all'intemperie, oltre ad offrire una qualità imbattibile.

Per informazioni: ***http://bit.ly/arloultraprezzo***

469 EURO

MOLTO PIÙ DI UNA BILANCIA

BEURER BF 700

Monitora non solo il nostro peso, ma anche altri valori utili per meglio comprendere se siamo in buona salute (quantità di massa grassa, percentuale di acqua, massa muscolare, massa ossea, indicatore calorico AMR/BMR). Tutti i dati vengono trasferiti tramite Bluetooth sul nostro smartphone e, grazie all'app gratuita HealthManager, possiamo tenere traccia di tutti i cambiamenti..

Per informazioni: ***http://bit.ly/bilanciasmart***

LA STAMPANTE DA TASCHINO

HP SPROCKET X7N08A

Una stampante fotografica portatile è quanto ci sia di meglio per stampare al volo uno scatto realizzato con la fotocamera del nostro smartphone. La tecnologia di stampa termica Zink offre un'elevata qualità e permette di stampare senza bordi. Il trasferimento dei file da stampare avviene tramite Bluetooth 3.0.

Per informazioni: ***http://bit.ly/2JbJLQi***

UNA SALA GIOCHI SEMPRE CON TE

SEGA GENESIS

Anni e anni di pomeriggi spesi nelle salette di videogiochi hanno partorito oggi, nel 2018, questo: una portatile arcade machine di 15 cm, dotata di 3 batterie, con schermo TFT di 2.5 pollici, per divertirci con ben 240 giochi, riesumati direttamente dai nostri ricordi di infanzia! Un sogno proibito di generazioni di ragazzini amanti dei videogames, che ora diventa realtà.

Per informazioni: *http://bit.ly/minicoinop*

24 EURO

IL PICCOLO RASPY

RASPBERRY PI ZERO WH

La scheda di prototipazione più amata dai maker si fa ancora più piccola con il modello Zero. Un modello, questo, in realtà già noto a molti, anche se questa volta, la presenza della lettera "W" denota un'aggiunta abbastanza interessante: questo modello integra infatti un adattatore wireless per la connessione Wi-Fi b/g/n e Bluetooth 4.0. La "H" invece indica che è già pre-saldato l'header della GPIO. Il processore rimane sempre un Broadcome BCM2835 da 1 GHz, così come la memoria RAM che rimane a 512 MB. Perfetto per realizzare una telecamera di sorveglianza low cost o per numerose altre applicazioni da veri maker.

Per informazioni: *http://bit.ly/2XTmNRh*

21 EURO

LA LAMPADINA SMART

XIAOMI YEELIGHT

La casa diventa sempre più smart. Elettrodomestici che si connettono a Internet, telecamere che possono essere controllare da remoto e... lampadine intelligenti che si controllano direttamente dallo smartphone. È il caso delle Yeelight, prodotte da Xiaomi, che possono essere gestite dal nostro device, tramite Wi-Fi e utilizzando l'app ufficiale. La lampadina LED è RGB, dunque possiamo settare il colore che preferiamo o quello che più si adatta alla situazione.

Per informazioni: *http://bit.ly/xiaomilampadina*

22 EURO

RISCALDAMENTO SMART

NEST LEARNING THERMOSTAT

Questo termostato Wi-Fi è controlla il sistema di riscaldamento della nostra casa rendendo il tutto più efficiente (di conseguenza, riduce i consumi ed ottimizza il riscaldamento). La temperatura può essere variata direttamente dal nostro smartphone Android e la sua installazione è banale: essendo compatibile con tutti i sistemi di riscaldamento europei, basta sostituirlo al nostro vecchio termostato ed è già pronto all'uso.

Per informazioni: *http://bit.ly/2Hu8OeW*

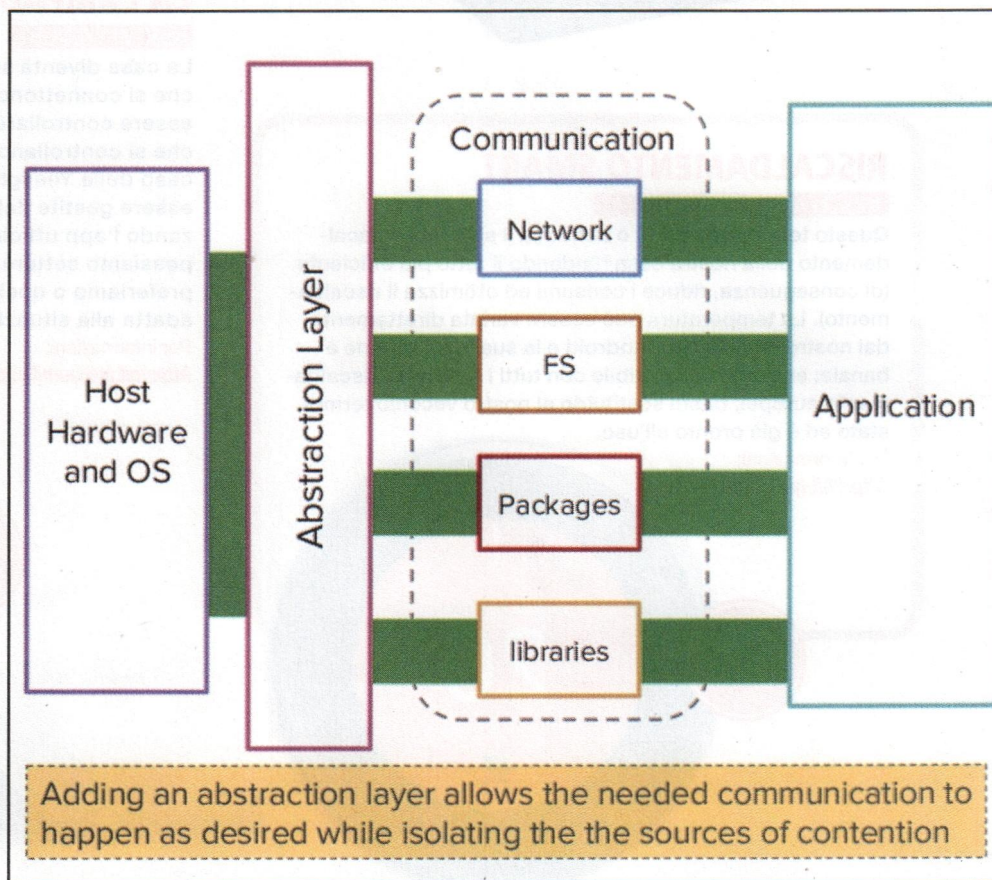
235 EURO

Macchine virtuali o container?

Per decenni la virtualizzazione si è sempre fatta tramite macchine virtuali, ma da diversi anni esistono i più snelli container. Vediamo assieme come e quando utilizzare l'una o l'altra tecnologia

Luca Tringali

Chiunque utilizzi un computer, anche a livello desktop, ha almeno sentito parlare delle macchine virtuali. Qualcuno ha sicuramente utilizzato una macchina virtuale, come VirtualBox, di solito per utilizzare qualche vecchio programma non più funzionante sui moderni sistemi operativi. Gli utenti più esperti, soprattutto quelli che si occupano di server, conoscono tuttavia anche un'altra tecnologia di virtualizzazione: i container. Negli ultimi anni i container sono stati oggetto di una forma di "hype", per cui tutti vogliono utilizzarli solo perché vanno di moda, senza pensare esattamente alle loro caratteristiche e quindi in quali casi potrebbe non essere una buona idea ricorrere a un container, affidandosi piuttosto a una "vecchia" macchina virtuale. Si tratta di un meccanismo molto comune, spesso capita che una particolare tecnologia venga impiegata molto solo per una sorta di "bolla", che prima o poi si sgonfia. La realtà è che i container risolvono alcuni (anche se non tutti) i problemi delle macchine virtuali, e possono davvero essere un ottimo modo per pubblicare le proprie applicazioni e installarle su dei server. Tuttavia, non possono garantire lo stesso livello di sicurezza di una macchina virtuale e vanno usati con molta cautela, ricordandosi che le proprie applicazioni devono essere sicure di per sé, invece di affidarsi soltanto al "potere contenitivo" del container come unica misura di sicurezza. Ma che cosa è un container? In poche parole, è una sorta di ambiente separato dal sistema operativo del proprio computer, e che può simulare condizioni differenti da quelle del sistema host. Il container non è una completa macchina virtuale, ma un "contenitore" che racchiude soltanto ciò che è strettamente necessario per far funzionare un singolo programma, risparmiando quindi molto spazio sul disco e molte risorse hardware. Sostanzialmente, non viene virtualizzato un intero computer, ma solo il sistema operativo. In effetti, non ha molto senso mettere in piedi una completa macchina virtuale, riservandole risorse come CPU e RAM,

Adding an abstraction layer allows the needed communication to happen as desired while isolating the the sources of contention

e replicare tutto il sistema operativo solo per far funzionare un singolo programma, che è quello che purtroppo spesso accade con le macchine virtuali. Prima di entrare nei dettagli delle differenze tra macchine virtuali e containers, però, conviene parlare di una tecnologia a metà strada. Analizziamo quindi una famosa pessima idea: le macchine virtuali Java.

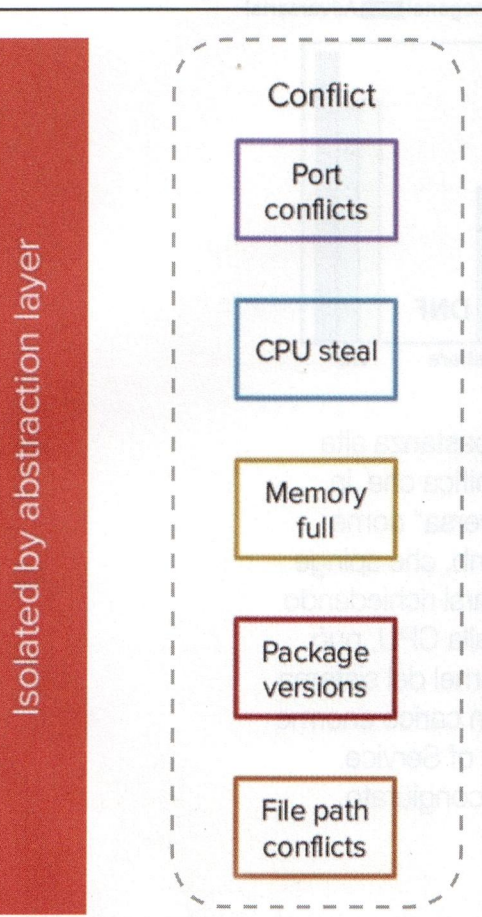
UN PRECEDENTE: IL TENTATIVO DI REALIZZARE UNA "VM LITE"

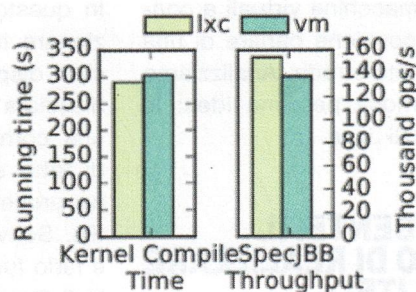
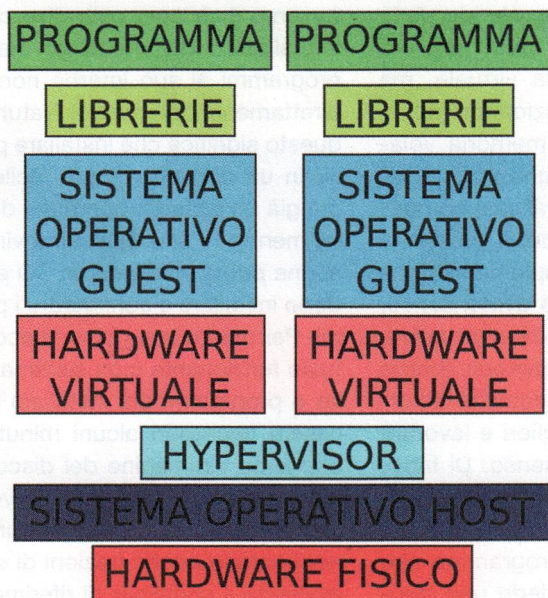
Java è un linguaggio di programmazione inventato nel 1992, con l'obiettivo di permettere ai programmatori di scrivere programmi capaci di funzionare su quanti più dispositivi possibile. L'idea era di compilare il codice non in uno specifico codice binario valido per un solo tipo di processore e sistema operativo ma in un "bytecode", una sorta di codice binario che gira su una macchina virtuale (che è per l'appunto la Java Virtual Machine).
In questo modo, è possibile far funzionare il proprio bytecode su qualsiasi dispositivo per il quale sia stata rilasciata una JVM. LA JVM non era una completa macchina virtuale, ma di fatto simulava il funzionamento di un processore e della memoria volatile. Scrivere il codice una volta sola, e farlo funzionare su qualsiasi computer? Sembrava fantastico. Il problema è sempre stato nell'implementazione e se negli anni '90 Java aveva senso, perché non c'erano molte alternative, oggi C++ e Python (magari con librerie grafiche cross-platform come le Qt) offrono risultati molto migliori e lavorare anche in Java non ha senso. Di fatto, un programma Java funziona come una sorta di libreria che viene caricata all'interno di un altro programma che è la JVM, la quale richiede una buona dose di risorse già da sola, ma alla fine non c'è una vera separazione tra la JVM e il resto del sistema operativo, quindi un programma può sfruttare bug nella JVM per danneggiare il sistema host. Infatti, le macchine virtuali Java portano con se una buona parte della complessità e del consumo di risorse di una vera macchina virtuale, ma senza il fondamentale vantaggio di una vera separazione dalla macchina fisica e dal sistema operativo host. Per questo sono una pessima idea, conservano la caratteristica peggiore e perdono quella migliore. I container fanno, almeno in teoria (il risultato dipende dall'implementazione), esattamente il contrario: consumano molte meno risorse, e mantengono la propria applicazione separata dal resto del sistema operativo host.

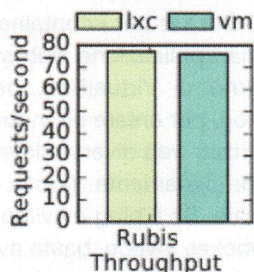
Fig. 1 - I container funzionano come un livello di astrazione per il sistema operativo, creando degli ambienti separati per evitare conflitti tra le varie applicazioni

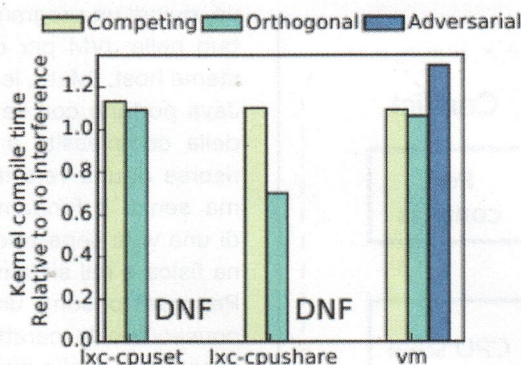
Isolated by abstraction layer
Conflict
Port conflicts
CPU steal
Memory full
Package versions
File path conflicts

LA DIFFERENZA TRA MACCHINE VIRTUALI E CONTAINERS

Quindi, qual è la differenza tra una macchina virtuale e un container? Per semplificare, possiamo dire che una macchina virtuale costituisce una sorta di hardware astratto, sul quale si può lavorare come se fosse un vero computer a se stante. Un container è invece una sorta di sistema operativo astratto. La macchina virtuale permette un accesso diretto all'hardware e alle varie risorse virtualizzate, mentre il container non lo permette perché tutto deve passare attraverso il sistema operativo che viene virtualizzato dal container stesso, e i programmi al suo interno non vedono direttamente l'hardware. Naturalmente, questo significa che installare programmi in un container è più facile perché c'è già un sistema operativo disponibile, mentre in una macchina virtuale bisogna prima installare un SO e appena dopo installare e configurare i programmi. Per creare una nuova macchina virtuale funzionante (con sistema operativo e programmi già installati) possono essere necessari alcuni minuti, anche copiando l'immagine del disco da una di riferimento già pronta. Invece, per creare una nuova istanza di un container bastano poche frazioni di secondo, avviando il container di riferimento con i giusti parametri. Facciamo l'esempio di VirtualBox per le macchine virtuali e di Docker per i containers: se abbiamo una applicazione web sviluppata all'interno di VirtualBox, per esempio un blog, per creare un nuovo blog a un indirizzo web diverso dovremo creare una completamente nuova macchina virtuale. Se il blog è sviluppato come app Docker, invece, basta avviare dal terminale un nuovo container specificando il nuovo indirizzo a cui deve rispondere il sito. Per esempio, ogni volta che accediamo a Google Docs, sul server di Google viene avviato un apposto container per fornire al nostro utente l'interfaccia web: usare macchine virtuali renderebbe l'avvio del servizio inutilmente lento. Quello che è importante capire è che i container non sono la soluzione magica a tutti i problemi, e le macchine virtuali non sono obsolete: sono due modi diversi per risolvere un problema simile, ma ciascuna delle due tecnologie può essere valida a seconda delle specifiche caratteristiche di cui abbiamo bisogno. Le macchine virtuali sono più sicure, ma i container sono più efficienti. Se vogliamo virtualizzare una sola applicazione, i container semplificano la vita, se vogliamo virtualizzare molte

MACCHINE VIRTUALI

Perché sceglierle...

(a) CPU intensive

I Linux Container (LXC) impiegano meno tempo e riescono ad eseguire un po' più operazioni al secondo rispetto alle macchine virtuali (VM). Il consumo di CPU è quindi un po' più efficiente con i container, ma la differenza non è così notevole.

(d) Network intensive

Le performances relative al traffico di rete degli LXC e delle VM sono molto simili, con i container in leggero vantaggio.

L'interferenza è abbastanza alta per i container. Significa che, in una situazione "avversa" come la classica fork-bomb, che spinge un processo a forkarsi richiedendo molta attenzione dalla CPU, può succedere che il kernel del sistema host si trovi sotto un carico enorme e risulti in un Denial of Service. Nelle VM il DoS è scongiurato.

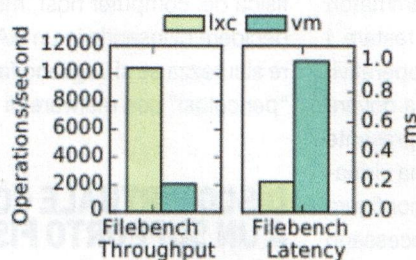
FONTE:
Prateek Sharma1,
Lucas Chaufournier1 ,
Prashant Shenoy1 ,
Y.C. Tay2
University of Massachusetts Amherst1,
National University of Singapore2
http://bit.ly/middleware16

CONTAINERS

PROGRAMMA

LIBRERIE LIBRERIE

SISTEMA OPERATIVO HOST

HARDWARE FISICO

(c) Disk intensive

I containers riescono ad eseguire molte più operazioni di lettura e scrittura su disco rigido, con meno millisecondi necessari. La differenza è così palese perché l'hypervisor delle macchine virtuali è un collo di bottiglia per le operazioni di I/O.

(b) Memory intensive

Al di là del fatto che i container occupano meno memoria, in media un mezzo o un terzo di una macchina virtuale, sono anche più efficienti nell'accesso sia in scrittura che lettura alla RAM, con un latenza inferiore.

Una buona soluzione a vari problemi è rappresentata dai "nested containers". Si crea una macchina virtuale, e al suo interno si inseriscono i container (più di uno). Questo permette di avere la sicurezza delle VM, senza però perdere troppe performance: come si può notare gli LXCVM eseguono operazioni in tempi minori rispetto alle VM e soltanto appena leggermente maggiori rispetto agli LXC puri. Tra l'altro, questo permette di virtualizzare anche sistemi operativi e architetture diversi da quelli del sistema host con cui funziona il server.

Da notare che il carico di lavoro dei container si rivela inferiore a quello delle VM per operazioni non troppo impegnative sulle immagini. Il comando apt-get dist-upgrade in un LXC è più lento che in una VM. Quindi, per aumentare l'efficienza, nell'immagine di un container bisogna mettere soltanto il minimo indispensabile.

applicazioni interconnesse tra loro è meglio usare una macchina virtuale.

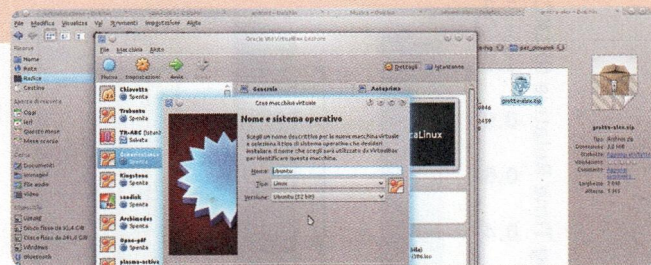
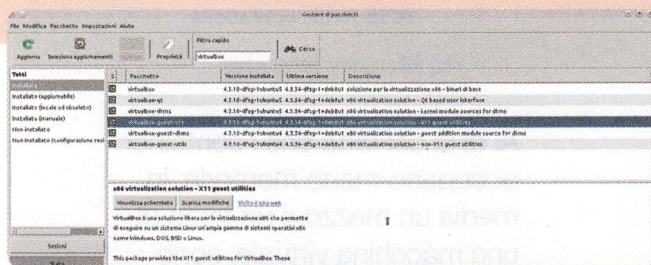
COME CONFIGURARE UNA VM A SECONDA DEL SISTEMA GUEST

Le macchine virtuali sono altamente configurabili, e questo permette di supportare un gran numero di applicazioni che, magari, funzionano soltanto su particolari sistemi o architetture. VirtualBox permette soltanto l'emulazione di processori x86 a 32 e 64 bit, ma altri virtualizzatori come QEMU consentono anche l'emulazione di diversi tipi di processori, come gli ARM che equipaggiano smartphone e Raspberry. In fondo, uno degli utilizzi principali che gli utenti comuni fanno di VirtualBox è l'avvio di particolari programmi che non funzionano su GNU/Linux o magari nemmeno su versioni recenti di Windows. Molti programmatori utilizzano macchine virtuali per testare i loro programmi su diversi sistemi operativi, per assicurarsi che tutto funzioni a dovere (lo stesso emulatore di Android presente nell'SDK di Google è una macchina virtuale). Ciò significa che quando si configura una nuova macchina virtuale è necessario considerare proprio di cosa si abbia bisogno. L'architettura del processore è la cosa più importante perché non avrebbe senso cambiarla in seguito (dopo aver installato il sistema operativo). Ma bisogna considerare anche la quantità di RAM, le accelerazioni grafiche, e la dimensione del disco rigido. Inoltre, in linea di massima è sempre consigliabile configurare la scheda di rete virtuale con un bridge sulla scheda fisica del computer host, ma si può anche decidere di inserirla in un NAT per maggiore sicurezza se si vogliono fare esperimenti "pericolosi" con malware di vario tipo.

DISCO VIRTUALE COLLEGATO A UN SUPPORTO FISICO

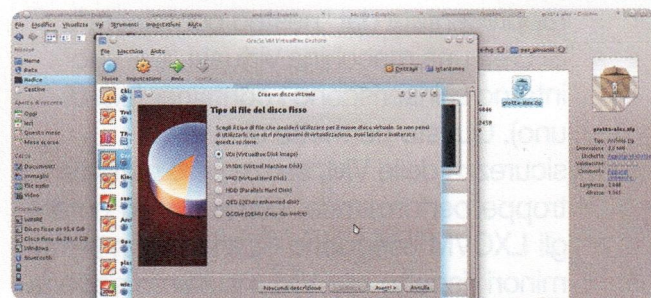
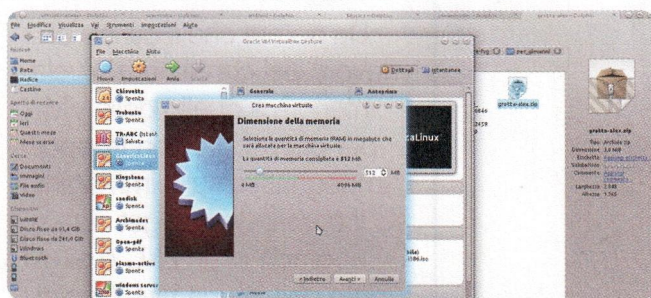
Quando si lavora con una macchina virtuale, il disco rigido è probabilmente la parte più importante perché è in esso che si installa il sistema operativo, e da questo dipende tutto il funzionamento della macchina virtuale. Quindi è importante poterli manipolare a proprio piacimento,

Primi passi con VirtualBox

Cominciamo a creare una nuova macchina virtuale

01 L'INSTALLAZIONE

Per prima cosa si deve ovviamente installare il programma Virtualbox, utilizzando il gestore dei pacchetti del proprio sistema. Oltre al pacchetto con i binari di base, è consigliabile installare anche i pacchetti guest, che contengono le **guest** additions.

02 MACCHINA NUOVA

Avviato Virtualbox possiamo vedere l'elenco delle macchine virtuali esistenti, oppure crearne una nuova cliccando sul pulsante **Nuova**. La prima informazione che ci viene chiesta è il nome della macchina ed il tipo di sistema guest che utilizzeremo.

03 ABBASTANZA RAM

Ovviamente, tutte le impostazioni potranno essere modificate in futuro. La seconda informazione che ci viene richiesta è la quantità di memoria RAM da riservare alla macchina virtuale che stiamo costruendo.

04 IL DISCO VIRTUALE

Il passo successivo consiste nel creare un disco rigido virtuale per la macchina che stiamo costruendo. Il file che conterrà il disco virtuale può essere di diversi tipi: di solito, si può utilizzare il formato VDI.

per semplificarsi la vita. Purtroppo, la gestione dei dischi virtuali di VirtualBox dall'interfaccia grafica del programma ha qualche limite. Vi sono un paio di trucchi che si rivelano spesso utili, ma che possono essere svolti soltanto da riga di comando utilizzando il programma VboxManage. Per esempio, è possibile creare un disco virtuale "fittizio" che rappresenta un disco reale connesso al sistema host. Per esempio, possiamo collegare al nostro computer un disco rigido esterno (che chiameremo **/dev/sdb**). A quel punto ci basta dare il comando

```
sudo  VBoxManage internalcommands
  createrawvmdk -filename /home/luca/
          disco.vmdk -rawdisk /dev/sdb
```

e otterremo il disco virtuale fittizio **/home/luca/disco.vmdk**. Ora possiamo inserire questo disco fittizio in una macchina virtuale ed utilizzarlo come se fosse davvero un disco di Virtualbox. Questo metodo è molto comodo anche per installare un sistema operativo su un altro computer: invece di accedere al computer in questione, basta rimuovere il suo disco rigido collegandolo tramite un adattatore USB, e installare il sistema operativo dal nostro pc tramite VirtualBox.

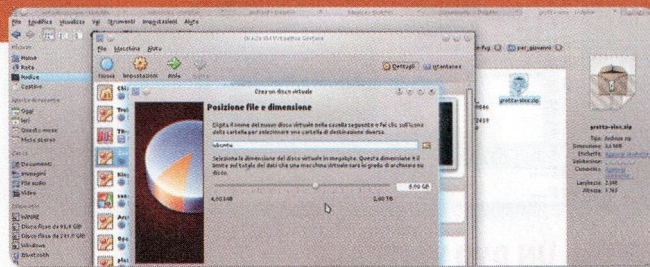
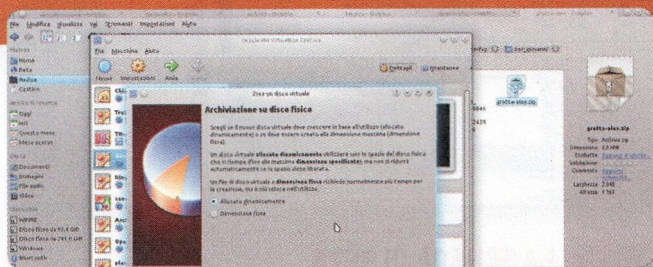
RIDIMENSIONARE UN DISCO

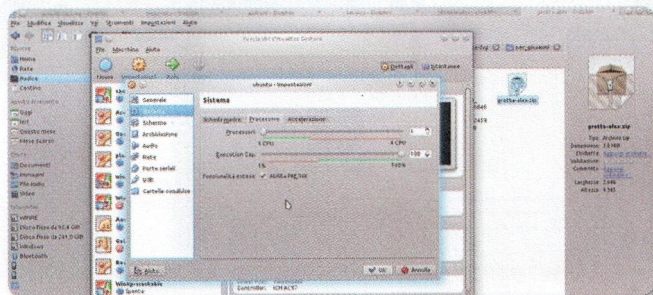
Un'altra attività utile consiste nell'espansione di un hard disk virtuale: magari ne avevato creato uno di soli 8GB, ma poi vi siete accorti che non erano sufficienti. Basta utilizzare il seguente comando:

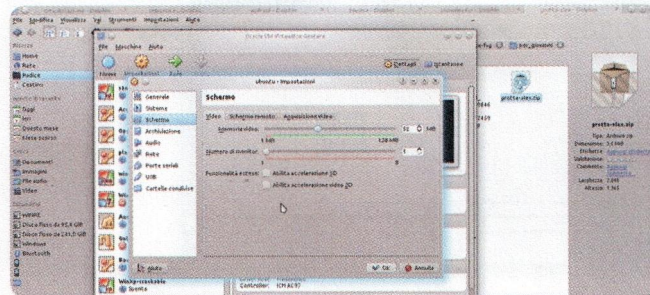
```
sudo VBoxManage modifyhd "disco.
                  vdi" --resize 30000
```

Dove **disco.vdi** è il disco virtuale da modificare e **30000** è la nuova dimensione in Mega Byte. Da notare che in questo modo è possibile soltanto aumentare la dimensione di un disco. Per ridurla bisogna prima di tutto entrare nel sistema guest e ridimensionare le partizioni spostandole in modo da avere spazio non allocato alla fine del disco. Poi si crea un nuovo disco (delle dimensioni pari a quelle dello spazio allocato sul disco originale). E alla fine si esegue una copia dei

Le impostazioni nel dettaglio

Costruiamo il disco rigido virtuale, scegliamo il processore e la memoria video

01 UN DISCO DINAMICO

È consigliabile che lo spazio del disco virtuale venga allocato in modo dinamico. Significa che se costruiamo un disco da 8 GB, il suo file non peserà subito 8GB: comincerà con un peso di pochi MB, ed aumenterà man mano che il disco virtuale viene riempito.

02 FILE E DIMENSIONE

Il disco virtuale, lo abbiamo detto, non è altro che un file. Dobbiamo quindi ora scegliere la posizione in cui salvare il file in questione, ed anche la sua dimensione massima. Sono supportati dischi virtuali fino a 2TB.

03 QUANTI PROCESSORI

La macchina virtuale è ora pronta. Possiamo selezionarla dall'elenco e cliccare sul pulsante **Impostazioni**. Ad esempio, possiamo modificare le impostazioni del **Sistema**, per scegliere il numero di core del processore ed eventuali funzioni.

04 LA SCHEDA VIDEO

Nella scheda **Schermo** è possibile decidere la memoria della scheda video virtuale. Si può anche abilitare l'accelerazione 3D e quella 2D, ma si tratta di opzioni che pesano molto sull'efficienza della macchina virtuale.

dati con il comando

```
sudo VBoxManage clonehd "disco.
  vdi" "nuovodisco.vdi" --existing
```

Si può poi usare la stessa macchina virtuale, sostituendo il vecchio HD virtuale con il nuovo.

ACCEDERE AI FILE DAL SISTEMA HOST

Può anche essere utile, a volte, montare sul sistema host una partizione del disco virtuale VDI, per accedere direttamente ai file della macchina virtuale. Si può usare il modulo nbd, con questi comandi:

```
sudo modprobe nbd
sudo qemu-nbd -c /dev/nbd0 ./
                    NewVirtualDisk1.vdi
sudo fdisk -l /dev/nbd0
sudo mount /dev/nbd0p2 /mnt
```

E la partizione sarà montata in **/mnt**. Poi è possibile smontare la partizione digitando

```
sudo umount /mnt
sudo qemu-nbd -d /dev/nbd0
```

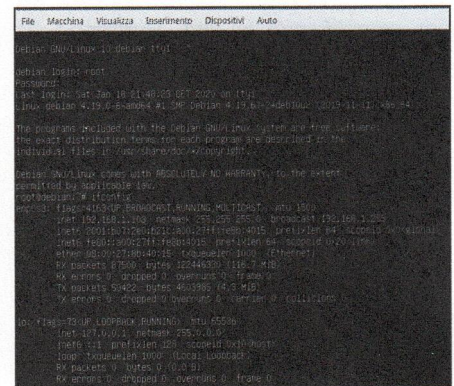
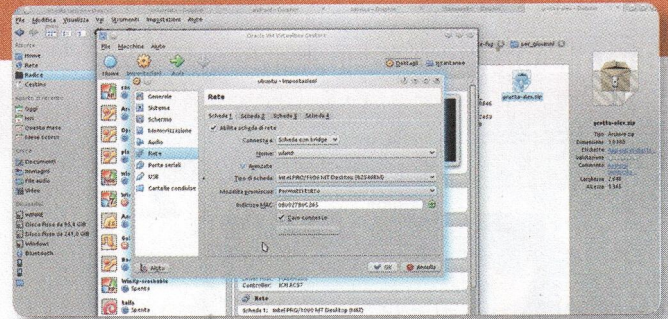
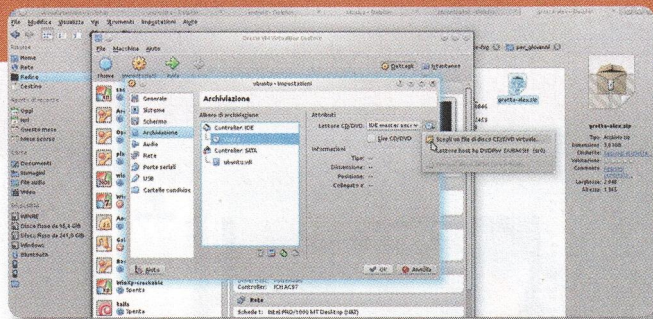
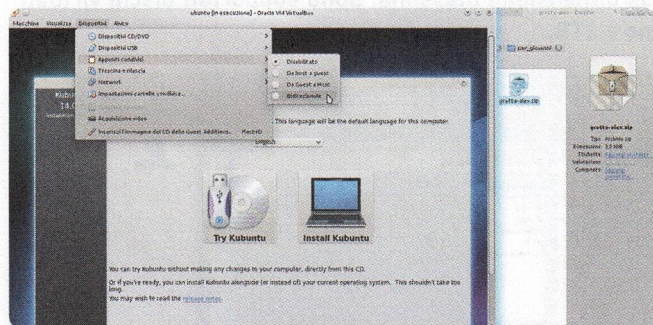
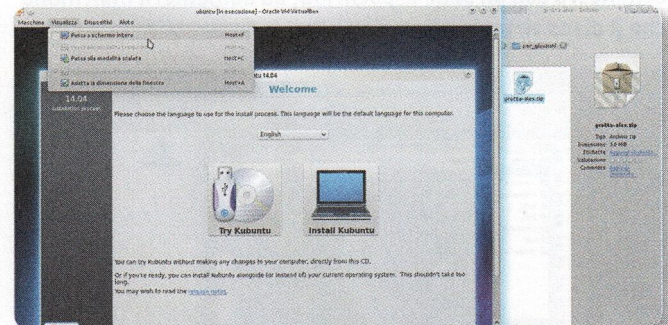



Fig. 3 - Per conoscere l'indirizzo IP della macchina virtuale basta suare il comando ifconfig oppure "ip a" dal suo terminale

La connessione ethernet

Impostiamo la scheda di rete e siamo pronti per provare la macchina virtuale

01 UN DVD VIRTUALE

La scheda **Archiviazione** ci permette di scegliere i vari supporti di memorizzazione. Per esempio, possiamo modificare il disco ottico predefinito: per simulare un disco ottico basta selezionare una immagine ISO (per esempio quella di Ubuntu).

02 LA SCHEDA DI RETE

La scheda **Rete** ci permette di scegliere la scheda di rete che vogliamo per la nostra macchina virtuale. Conviene sempre scegliere una **Scheda con bridge**, ed eventualmente abilitare la **modalità promiscua**, per sniffare i pacchetti della rete.

03 APPUNTI CONDIVISI

È possibile trasferire informazioni tra la macchina reale e quella virtuale condividendo gli appunti: dopo avere avviato la macchina virtuale, basta scegliere il menù **Dispositivi/Appunti condivisi/Bidirezionale**.

04 A TUTTO SCHERMO

Quando la macchina virtuale è avviata e funzionante, possiamo ottenere maggiore comodità mettendola a tutto schermo. Per farlo basta premere contemporaneamente il tasto della lettera **F** ed il tasto "host", che di solito corrisponde al tasto **Ctrl** posizionato a destra.

Riassumendo: LE MACCHINE VIRTUALI

PRO

- Si può dotare di un proprio sistema operativo, per la massima personalizzazione
- Si possono modificare i programmi installati sulla macchina virtuale, andando avanti per molti anni con la stessa VM di partenza semplicemente facendole aggiornamenti e modifiche
- La macchina virtuale è completamente separata dal sistema host

CONTRO

- Dover installare un sistema operativo richiede alcuni GB di spazio, il che è uno spreco visto che le applicazioni di per se pesano raramente più di 1GB con tutti i file accessori
- Se si vuole creare un'altra virtual machine partendo da una VM già esistente (per esempio per avere due server web) bisogna copiare tutti i file, si occupa il doppio dello spazio e ci vuole molto tempo per inizializzare la nuova VM.
- Mantenere correttamente aggiornato il sistema guest di una macchina virtuale è scomodo, è come dover aggiornare un vero computer, mentre con un container basta scaricare la nuova immagine del container stesso
- Distribuire una propria applicazione in una macchina virtuale è scomodo e costoso, con un container la distribuzione è molto più facile
- Riservando RAM e CPU per ogni macchina virtuale, anche con i sistemi di ottimizzazione forniti da hypervisors come KVM, si rischia di sprecare risorse anche quando non è necessario perché una app non sta davvero facendo qualcosa, mentre in un container le risorse vengono usate solo quando è davvero necessario

Riassumendo: I CONTAINERS

PRO

- Occupa poco spazio sul disco rigido e poca RAM
- Per creare un nuovo servizio partendo da uno già esistente, basta avviare lo stesso container con parametri diversi (per esempio, due server web devono funzionare su porte TCP diverse)
- Aggiornare il container è semplice e veloce, basta scaricare la nuova immagine

CONTRO

- Ha bisogno di un sistema operativo host che svolga tutte le operazioni di base
- Non si possono cambiare i programmi che sono stati inseriti nel container dopo la sua creazione, bisogna crearne un altro
- Tutti i container devono supportare il sistema host su cui vengono installati (cosa in linea di massima sempre vera, ma in alcuni casi può essere un problema)
- I container non separano completamente il proprio interno dal sistema host: i file presenti nelle cartelle /dev e /sys sono solitamente accessibili dall'interno del container. Questo può essere pericoloso, se l'applicazione all'interno del container riesce a ottenere privilegi di amministrazione. Si può risolvere con una apposita configurazione, ma bisogna prestarvi attenzione
- Le applicazioni devono essere pacchettizzate in vari containers, con tutte le loro dipendenze, e alcuni containers possono dipendere l'uno dall'altro. Con tante applicazioni da gestire, può essere complicato evitare conflitti. In linea di massima, i container vanno bene se si vuole virtualizzare una sola app per volta.

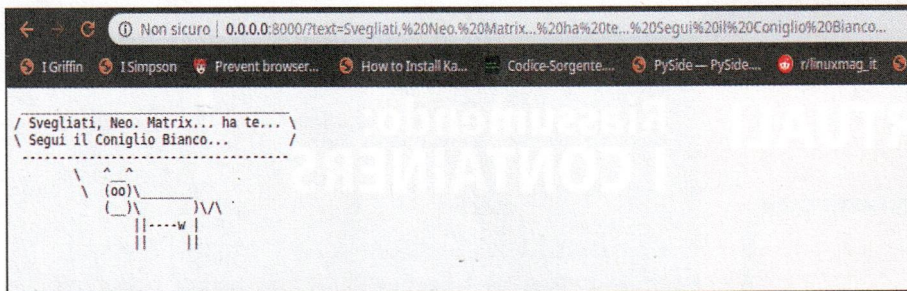



Fig. 2 - L'accesso all'app del container avviene tramite l'URL http://0.0.0.0:8000/?text=Testo

DISTRIBUIRE LE PROPRIE APPLICAZIONI IN UN CONTAINER: DOCKER

Chi vuole creare una propria immagine Docker per pubblicare una applicazione può cominciare scrivendo un file chiamato **Dockerfile**:

```
FROM python:3-slim-buster
```

La prima riga indica l'immagine di partenza: si può scegliere qualsiasi cosa, in linea di massima conviene partire in piccolo e poi aggiungere il necessario. L'immagine **python** offre l'interprete Python e il gestore delle librerie PIP preinstallato. Il tag **3-slim-buster** indica che questa versione dell'immagine è basata su Debian Buster in versione minimale (slim), con Python3 invece dell'ormai vecchio Python2.

```
EXPOSE 8000
```

Siccome lavoriamo con un server dobbiamo poter accedere alla sua porta dall'esterno del container. Nel nostro esempio usiamo la porta 8000 per il server web, ma si può scegliere quella che si vuole.

```
RUN pip install --upgrade pip
RUN apt-get update
```

L'immagine da cui siamo partiti potrebbe essere vecchia: i database di PIP e di APT devono essere aggiornati. Con l'istruzione RUN possiamo dire a Docker di eseguire dei comandi nel container appena creato.

```
RUN apt-get install -y nano cowsay
```

Dopo che APT è aggiornato possiamo procedere a installare i componenti di cui abbiamo bisogno. Per il nostro esempio serve solo cowsay, però avere anche l'editor di testi Nano può essere utile per il debug.

```
RUN adduser --disabled-password
                          --gecos "" worker
USER worker
WORKDIR /home/worker
```

In linea di massima, è una buona idea far eseguire la propria applicazione da un utente non root, in modo da avere un primo livello di protezione nel caso la nostra app contenga bug che permettono a un attaccante di ottenere una shell. Il primo comando crea l'utente di sistema **worker**, senza password e senza opzioni personali (gecos è impostato come testo vuoto). Poi si suggerisce a Docker che i prossimi comandi dovranno essere dati dall'utente appena creato, lavorando dentro la sua cartella home.

```
ENV PATH="/home/worker/.local/
                        bin:${PATH}"
```

È importante aggiungere alla variabile d'ambiente, per i vari script che vorremo eseguire, la cartella in cui vengono installate le librerie di Python.

```
COPY --chown=worker:worker require
              ments.txt requirements.txt
RUN pip install --user -qr require
                              ments.txt
```

A questo punto si può copiare il file **requirements.txt**, che contiene la lista dei pacchetti da installare tramite PIP per le varie librerie necessarie. Nel programma di esempio serve solo la libreria **Flask**. Eseguendo il comando **pip install** con l'opzione **r** vengono installate ricorsivamente anche i vari requisiti.

```
COPY --chown=worker:worker server.py .
```

Ormai mancano solo i file dell'applicazione: nel caso dell'esempio c'è solo il file **server.py**, ma non ci sono limiti sul numero di file e cartelle da copiare dentro il container.

```
CMD ["python3", "./server.py"]
```

L'ultima istruzione è l'impostazione del comando da eseguire all'avvio del container: è il comando che ci permette di avviare l'applicazione web.

COMPILARE L'IMMAGINE DOCKER

Realizzato il file Docker, e testato il proprio programma, bisogna creare l'immagine. Il comando, da dare nella cartella del file **Dockerfile**, è molto semplice:

```
sudo docker build -t cowsay .
```

Saranno necessari alcuni minuti: prima di tutto viene scaricata (se non è già presente) l'immagine base, poi viene creata una immagine nuova con il nome specificato (cioè **cowsay**) e eseguiti al suo interno tutti i comandi che abbiamo previsto.
Si può verificare che l'immagine sia stata creata e aggiunta all'elenco dei propri container con il comando:

```
sudo docker images
```

che fornirà un risultato di questo tipo:

```
REPOSITORY    TAG       IMAGE ID
cowsay   latest  326387cea398
```

Finita la costruzione dell'immagine possiamo provare a avviarla col comando

```
sudo docker run --rm -it -p
                    8000:8000 cowsay
```

È importante specificare il forwarding delle porte: la prima porta indicata è quella che sarà visibile dal sistema host, la seconda è quella del sistema interno al container. Per esempio, si potrebbero lanciare altre istanze del container con i comandi

```
sudo docker run --rm -it -p
              8001:8000 cowsay
sudo docker run --rm -it -p
              8002:8000 cowsay
```

In modo da avere sul proprio sistema host tre diversi server, che rispondono sulle porte "esterne" 8000, 8001, e 8002. La porta interna è sempre la stessa perché è quella specificata nel codice del nostro programma e nel Dockerfile.
Da considerare che l'opzione **--rm** permette la pulizia automatica del filesystem dopo lo stop del container, così da non occupare spazio inutilmente. Ma se si fa del debug è bene toglierla, così da avere tutti i file anche interrompendo bruscamente l'esecuzione del container, per capire cosa sia andato storto.
Sempre per eseguire il debug quando qualcosa non funziona, si può lanciare l'immagine del container con il comando

```
sudo docker run --rm -it -p
         8000:8000 cowsay bash
```

In questo modo l'immagine viene avviata, ma viene eseguito il comando **bash** invece di quello previsto nel **Dockerfile** al termine del caricamento dell'immagine stessa. Si ottiene quindi un terminale dentro il container, per provare a lanciare manualmente la propria applicazione e leggere i messaggi d'errore. Quando l'immagine è ritenuta pronta alla distribuzione, si può fare un backup in formato tar col comando **save**:

```
sudo docker save --output cowsay.
                      tar cowsay
```

Con questo stesso metodo è stata realizzata l'immagine di esempio, che si trova nel DVD allegato a questo numero di GNU/Linux Magazine. Per caricare questa immagine in un altro sistema è sufficiente usare il comando load, specificando il nome dell'archivio tar:

```
sudo docker load --input cowsay.tar
```

Ovviamente, questo è anche il modo giusto di importare proprio l'immagine di esempio che forniamo nel DVD.

CREARE UNA IMMAGINE BASE PER DOCKER

La potenza di Docker sta nella possibilità di personalizzare i propri container, senza però dover necessariamente cominciare da capo ogni volta: quando si crea una immagine, è possibile scegliere una immagine "genitore" (parent image) dalla quale ereditare tutta la struttura di base del sistema operativo. Sono già disponibili immagini di Debian, Ubuntu e altre distro, "vanilla" oppure con alcuni programmi già installati. Ma è anche possibile creare le proprie immagini partendo da **scratch**, una installazione minimale di Linux che occupa pochissimo spazio. Basta creare un **Dockerfile** con questo contenuto:

```
FROM scratch
ADD hello /
CMD ["/hello"]
```

Con la direttiva **ADD** è possibile aggiungere all'immagine i propri programmi (che devono essere stati compilati precedentemente) e i file di configurazione. L'immagine così creata può poi a sua volta essere usata come base per creare altre immagini. Se diamo una occhiata alle immagini disponibili, per esempio quelle dotate di Python (***https://hub.docker.com/_/python***), ci accorgiamo che ne esistono molte versioni diverse. Esistono la 3-alpine, la 3-slim-buster, e la 3-buster. La prima è la più leggera, si tratta di un sistema davvero minimale, ed è consigliabile solo se davvero non si ha bisogno di nulla di più dell'interprete Python. La **slim buster** è una versione di Debian dotata praticamente solo del necessario per far funzionare il sistema di pacchetti APT: è comoda quando si vuole installare qualche programma eseguibile, e spesso è il migliore compromesso. La versione **buster** è la più pesante, occupa almeno 1GB, ma offre un vantaggio: i suoi componenti possono essere condivisi con le altre immagini che creeremo, quindi in realtà questa soluzione permette di risparmiare spazio. Questo è un dettaglio da tenere in considerazione anche quando si crea una propria immagine base: va bene tenersi leggeri, ma bisogna trovare il giusto compromesso per facilitare il riutilizzo delle parti comuni di un sistema.

Fig. 4 - L'accesso all'app della macchina virtuale avviene tramite l'URL http://IPdellaMacchina:8000/?text=Testo

VIRTUAL MACHINE E CONTAINER: L'ESEMPIO

Nel lato B del DVD allegato a questo numero di GNU/Linux Magazine forniamo una semplice applicazione web, che riceve un testo in input e fornisce un'immagine ASCII art con una mucca che pronuncia il testo. La stessa applicazione è presente sia in un container (**file cowsay.tar**) che in un disco per macchina virtuale (**cowsay.vdi**). I file servono a fare un semplice confronto tra le due implementazioni: si può infatti notare subito che lo spazio occupato è diverso. L'immagine del container richiede appena 260MB, mentre il disco della macchina virtuale occupa 1,8GB. Inoltre, se vuole avviare più di una istanza dell'applicazione web con Docker non serve copiare l'immagine, mentre con VirtualBox il disco deve essere clonato. Non c'è dubbio, il container occupa meno spazio. Però la macchina virtuale è molto più personalizzabile. E, soprattutto, sicura. Su una macchina virtuale è infatti molto semplice abilitare aggiornamenti automatici e garantire la protezione del sistema host.

La prima rivista scritta dai v

Un nuovo notebook? Bastano 400 euro!

Devi acquistare un portatile ma il tuo budget è limitato? Nessun problema! Con 400 Euro circa puoi ottenere un device di buone prestazioni per la tua Linux box e la programmazione

Non si devono temere a priori i notebook con prezzi convenienti, poiché già a partire da 300 Euro, è possibile ottenere dispositivi come si deve che per numerosi utenti offrono prestazioni sufficienti. Anche disponendo di un budget contenuto, la scelta è molto ampia: il test comparativo ha preso in esame modelli ultracompatti da 13 pollici fino ad arrivare a notebook di grande formato da 17 pollici. Tra i modelli testati è presente anche un convertibile, utilizzabile a scelta come notebook o tablet. In questa fascia di prezzo, è molto importante esaminare attentamente il dispositivo, poiché i produttori tendono a risparmiare parecchio sui notebook economici. Tutto questo può rivelarsi fastidioso e talvolta il dispositivo potrebbe risultare troppo lento o, ad esempio, offrire una breve autonomia, ma se il produttore ha armonizzato abilmente tutti i componenti hardware del dispositivo, non dovrebbero esserci problemi.

SE È PICCOLO, SI VIAGGIA MEGLIO

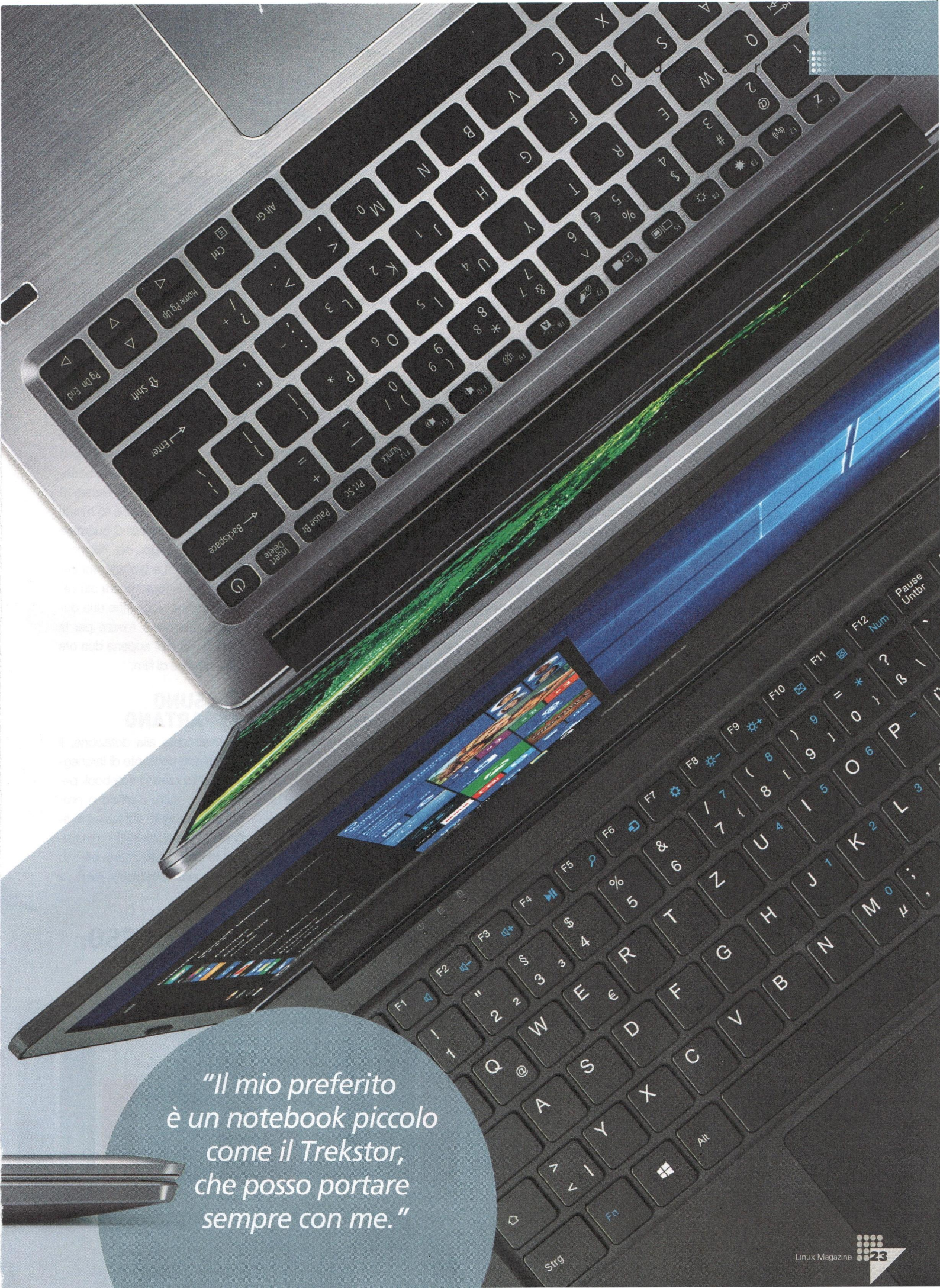
Lo chassis di questi notebook offre al produttore numerose possibilità di risparmio, che riguardano generalmente il peso del dispositivo. Tutto questo si nota con i notebook di grande formato, quando vengono utilizzati in mobilità: il modello da 17 pollici Asus Vivobook 17 pesa ben 2.163 grammi, mentre i notebook da 15 pollici di Dell, HP e Lenovo presentano un peso leggermente inferiore a 2 chilogrammi. Non pesano come dei mattoni, ma sono decisamente più pesanti dei modelli più piccoli da 13 e 14 pollici. Il Trekstor Surfbook pesa 1.229 grammi, mentre tra i modelli da 14 pollici, il più leggero si rivela il Medion Akoya E4251 con un peso di 1.338 grammi. Apprezzabile che gli alimentatori non siano particolarmente voluminosi e il più pesante del test vanta un peso di soli 315 grammi. Questi modelli non richiedono una borsa extra per il trasporto e spesso è sufficiente una semplice custodia imbottita.

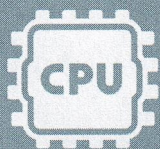
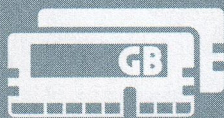
SCHERMI FULL HD QUASI PER TUTTI

I produttori tendono a risparmiare anche sul display, ma non in modo così esagerato come avveniva in passato: tranne un modello, tutti i display offrono la risoluzione Full HD (1.920 x 1.080 pixel). Solo l'Asus vanta un display da 17 pollici con risoluzione di 1.600x900 pixel: un formato abbastanza grande, ma poco ricco di dettagli per le foto e un po' pixelloso nella riproduzione dei caratteri. Relativamente alla fedeltà cromatica, tutti i modelli sono migliorabili e solo due notebook riproducono colori fedeli: il Trekstor e l'Asus. Gli altri sei esemplari hanno ottenuto la valutazione "molto scarsa" per la fedeltà cromatica. Chi non necessita di elaborare foto e video noterà generalmente questa carenza in una riproduzione cromatica leggermente pallida. Con quattro notebook, l'utente dovrebbe prestare particolare attenzione al display, poiché la qualità degli schermi di Asus, Dell, HP e Lenovo dipende moltissimo dall'angolo di visione. Chi guarda lo schermo leggermente di traverso, vedrà un'immagine più scura e da un'angolazione più estrema anche i colori vengono riprodotti in modo alterato. Solo l'Acer Swift 3 e il Medion Akoya E4271 offrono un display lucido con colori leggermente più saturi (ma con più riflessi sulla superficie).

DIFFERENZE DI VELOCITÀ

Cinque notebook sono equipaggiati con un piccolo processore Intel (Pentium Silver N5000), ma le differenze relative alla velocità di lavoro sono piuttosto consistenti. Questi cinque modelli mostrano quanto sia importante poter disporre di un notebook in grado di gestire i dati velocemente. L'hard disk del Vivobook rallenta talmente il processore, che i programmi LibreOffice girano ad una velocità dimezzata rispetto ai due dispositivi di Medion e al notebook di Dell, dove sistema operativo e software sono installati su un SSD. Tra questi modelli si posiziona il notebook di Trekstor con la sua memoria eMMc, una scheda fissa integrata nell'elettronica di comando, che funge da SSD. Anche questa memoria tende a rallentare la velocità, ma non in modo esagerato: il Surfbook si rivela comunque più lento del 15 percento. Nell'uso quotidiano, un processore leggermente più potente non significa poter goder di un maggior comfort: la maggior potenza offerta dal Pentium 4417U dell'Acer non viene avvertita dall'utente. Decisamente più veloce di tutti gli altri notebook, è solo l'HP 255 G7 dotato di processore AMD Ryzen 3 2200 U. Anche il Lenovo è equipaggiato con un processore AMD, ma si

■ Il Medion Akoy E4271 presenta una tecnologia moderna che offre due porte USB-C

“Il mio preferito è un notebook piccolo come il Trekstor, che posso portare sempre con me.”

CHECK LIST COSA SI OTTIENE CON 400 EURO

Processore
A bordo della maggior parte dei dispositivi è presente un Pentium N5000, che offre una velocità adeguata per i classici lavori d'ufficio. Solo raramente la velocità è più elevata: ad esempio, se nel notebook è installato un Ryzen 3.

RAM
4 Gigabyte sono (purtroppo) ormai standard. In questa fascia di prezzo, una RAM da 8 Gigabyte è rara. Apprezzabile che il notebook consenta di espandere la memoria.

SSD come storage
Con 400 Euro dovrebbe essere possibile ottenere un SSD da 119 Gigabyte, ma ancor meglio sarebbe un'unità da 238 GB. Nell'utilizzo quotidiano, un hard disk tradizionale tende a rallentare l'intero sistema.

WLAN e Bluetooth
Una connessione WLAN-ac e il sistema Bluetooth sono ormai d'obbligo. Questi notebook non possono offrire niente di meglio. I modelli privi di queste tecnologie sono antiquati ed è bene starne alla larga.

tratta di un antiquato Athlon A9-9425 che lavora addirittura un po' più lentamente del Pentium della concorrenza. Con programmi avidi di risorse, ad esempio per il videoediting, i notebook economici vengono sottoposti a uno stress eccessivo. Anche l'HP, notebook più veloce del test, mostra i suoi limiti e, quindi, gli utenti che necessitano di molta potenza è preferibile che si orientino verso un notebook più costoso come ad esempio l'Acer Swift 3 2019 (SF314-55G - ***http://bit.ly/acerswift32019***). Tutto questo è evidenziato nel confronto (in alto a destra) con il piccolo Acer Swift 3, incluso in questa comparativa. Il notebook di HP si rivela al top anche con i giochi, poiché pur con una risoluzione ridotta (1.366 x 768 pixel), riesce comunque ad offrire una velocità di 16 fps, un po' scarsa però per giocare in modo fluido. I modelli concorrenti equipaggiati con processori Intel si rivelano molto più lenti e la riproduzione dei giochi assomiglia ad una presentazione di diapositive.

QUASI SEMPRE SILENZIOSI

Un vantaggio offerto da processori meno potenti, è il ridotto consumo energetico: il Pentium N5000 richiede a pieno carico solo 6 Watt e per raffreddare il sistema è sufficiente un normale dissipatore. Quattro candidati al test (Dell, entrambi i modelli di Medion e Trekstor) sono privi di ventole e lavorano quindi in modo estremamente silenzioso. Con gli altri quattro modelli, la rumorosità delle ventole integrate si avverte solo raramente. Anche l'HP, che si rivela il notebook più rumoroso (1,1 Sone), non infastidisce l'utente. Con un utilizzo normale, la rumorosità delle ventole a bordo di Acer, Asus, HP e Lenovo (da 0,1 a 03 Sone) è appena percepibile.

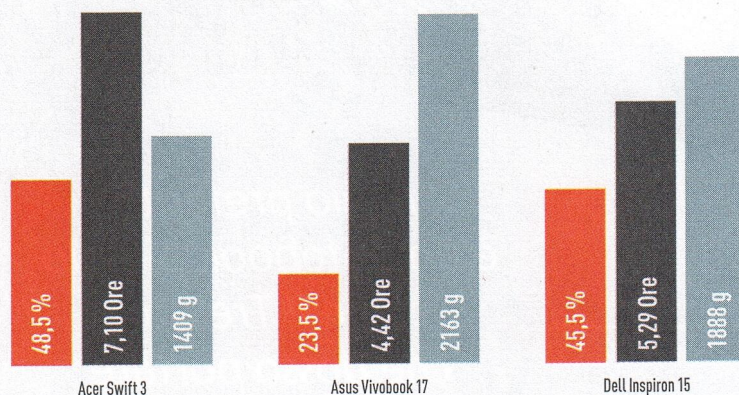
Grazie ad un touchscreen ruotabile sul retro della tastiera, il Medion Akoya E4271 può essere utilizzato come tablet

AUTONOMIA SPESSO ELEVATA

Un altro punto forte, ottenibile generalmente grazie ad un minor consumo energetico, è che la batteria riesce a fornire un'autonomia più lunga, purché il produttore resista alla tentazione di installare una batteria di minor capacità come offerto dal Surfbook che, nonostante sia equipaggiato con un processore molto parsimonioso, fornisce un'autonomia di solo tre ore. I due modelli di Medion dotati dello stesso processore, vantano invece due ore in più di autonomia. L'Aspire 3 è l'unico notebook che non necessita di avere una presa di corrente sempre a portata di mano, poiché offre una durata di ben sette ore per la produttività e di oltre sei ore per guardare film. Questa autonomia si rivela sufficiente per guardare i due primi film della trilogia "Il Signore degli Anelli" (ma non le Extended Edition!). I due notebook dotati di processore AMD non sono in grado di competere con l'Acer Swift 3, dato che la batteria dell'HP necessita di essere ricaricata dopo tre ore e 45 minuti di utilizzo e consente di guardare solo un episodio del "Signore degli Anelli". La batteria del Lenovo si esaurisce ancora più velocemente, poiché offre una durata di due ore e mezzo per la produttività e di appena due ore per la visione di film.

NESSUNO È SPARTANO

Relativamente alla dotazione, il prezzo non consente di largheggiare. Utilizzando i notebook per lavori con suite d'ufficio o programmazione, la dotazione si rivela sempre come si deve e quasi tutti i candidati al test offrono componenti hardware simili a

VELOCITÀ, AUTONOMIA, PESO:

quelli riportati nel box "Cosa si ottiene cono 400 Euro". Come "regalino", HP e Lenovo offrono addirittura un'unità DVD integrata. Tutti gli altri candidati al test necessitano di lettori DVD esterni, in vendita a prezzi estremamente contenuti (***http://bit.ly/lettoriesterni***). Al momento dell' acquisto di uno di questi notebook, il budget a disposizione potrebbe consentire anche di acquistare altri accessori.

IDONEI ANCHE PER GLI "SCRITTORI"

L'Acer e i dispositivi di Medion dimostrano che tastiera e touchpad dei notebook economici non devono per forza essere componenti di plastica di pessima qualità. L'Akoya E4271 consente all'utente anche di digitare direttamente sul display e, inoltre, grazie al suo touchscreen, è possibile utilizzare il notebook come tablet (vedi box). Con i restanti cinque candidati al test, è consigliabile che gli acquirenti eseguano prove di scrittura con la tastiera poiché, ad esempio, i tasti dell'HP si rivelano un po' ruvidi. Sui modelli di formato più grande, dotati di tastierino numerico extra, gli utenti di PC dovranno un po' adattarsi, poiché a causa dello scarso spazio disponibile per la tastiera rispetto a quella di un PC, i tasti del notebook sono più piccoli e più ravvicinati.

È POSSIBILE UN UPGRADE?

Un notebook economico dovrebbe uscire dalla fabbrica già adeguatamente equipaggiato e soprattutto la RAM, dovrebbe rivelarsi sufficiente per tutti gli utilizzi, poiché la metà dei candidati al test non consente di espandere la memoria. L'HP offre una RAM molto abbondante, che può arrivare fino a 32 Gigabyte. Sui notebook di Medion e sul Trekstor, è possibile installare agevolmente un SSD di maggior capacità e, a tal scopo, dispongono di un coperchio ad hoc per la manutenzione. Gli utenti che intendono potenziare il notebook dovranno rimuovere lo chassis, ma questa operazione non è indicata per i principianti, tuttavia non serve neppure la bacchetta magica.

QUALI PORTE OFFRONO?

Tutti i notebook testati offrono due veloci porte USB per un SSD o hard disk esterno, una porta combi per le cuffie o un headset, nonché una uscita HDMI, che consentirà di collegare velocemente un monitor, per poter disporre di un secondo display. Solo cinque modelli consentono il collegamento di un monitor con un semplice cavo HDMI, mentre per l'Akoya E4251 e per il Surfbook è necessario un adattatore per mini-HDMI o un cavo speciale con un connettore mini-HDMI. L'Akoya E4271 vanta invece una DisplayPort tramite USB-C, che consente di collegare più facilmente un monitor dotato di ingresso USB-C. Chi vuole collegare un numero più elevato di periferiche, è consigliabile che consulti questa comparativa. Ad esempio, tre notebook (Asus, HP e Lenovo) offrono una porta per cavo Ethernet.

COSA SI OTTIENE CON 1.000 EURO E PIÙ...

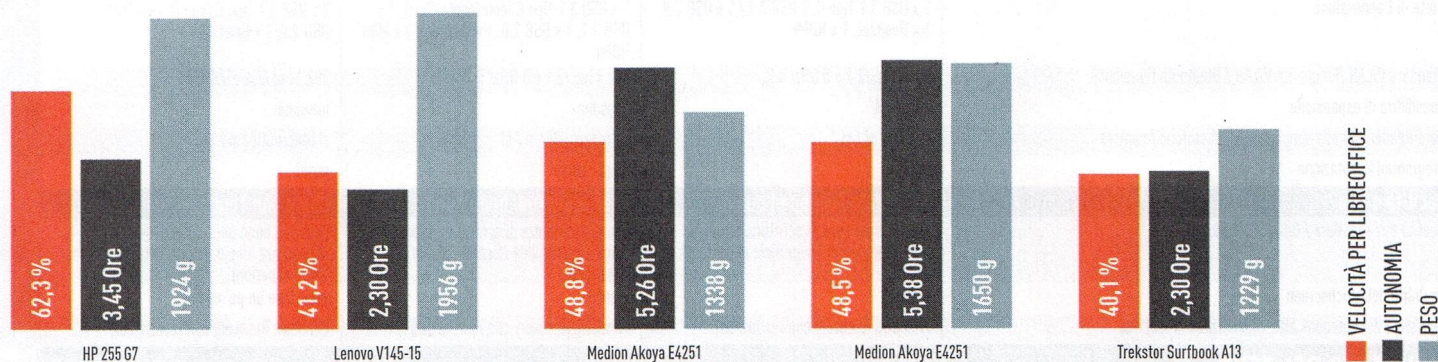
Chi acquista un notebook da 400 Euro non può logicamente aspettarsi un equipaggiamento portentoso. Il confronto con l'Acer Swift 3 2019, mostra quanto siano grandi le differenze con un modello da 1.000 Euro.

	ACER SWIFT 3 2019 (SF314-55G) 1.000 Euro http://bit.ly/acerswift32019	**ACER** SWIFT 3 (SF314-54-P2RK) 440 Euro
Velocità	Potenza sufficiente per l'ufficio, video-editing e giochi	La velocità è sufficiente per il lavoro d'ufficio, ma non per i giochi
Display	Display al top: ricco contrasto, nitido, riproduzione cromatica fedele	Display ricco di contrasto con scarsa fedeltà cromatica
Autonomia	Al top: quasi 8 ore per la produttività e 9 ore per guardare video	Piuttosto buona: 7 ore per la produttività, 6 ore per guardare video
Dotazione	RAM adeguata, SSD più capiente (477 GB), un numero sufficiente di porte di connessione	RAM scarsa, SSD piccolo (119 GB), un numero sufficiente di porte di connessione
Qualità costruttiva	Chassis in alluminio, pregiata qualità costruttiva, pesante	Chassis in plastica, ma di buona costruzione

CONCLUSIONI

L'Acer Swift 3 (440 Euro) si rivela indiscutibilmente il vincitore del test e per poco non ha ottenuto la valutazione "buono", dato che in questa fascia di prezzo nulla è scontato! Acer offre un mix di caratteristiche e prestazioni che non fa una piega. Per numerosi utenti è importante poter disporre di un display come si deve e di una velocità adeguata per LibreOffice e, inoltre, lo Swift 3 lavora in modo estremamente silenzioso ed offre un'autonomia piuttosto lunga. Il Trekstor Surfbook A13, vincitore del rapporto qualità/prezzo, si rivela un notebook ancora più economico, più piccolo e più leggero, ma gli acquirenti dovranno accontentarsi di un'autonomia e di una dotazione inferiore a quella di altri candidati.

Le differenze di prezzo sono minime, ma piuttosto consistenti relativamente a velocità, autonomia e peso. HP si rivela il più veloce, Acer offre l'autonomia più lunga e il più leggero del test è il Trekstor.

NOTEBOOK ECONOMICI

1 ACER SWIFT 3 (SF314-54-P2RK)

Prezzo: 440 Euro
http://bit.ly/as3prezzo

Il vincitore del test dimostra che un notebook da circa 400 Euro è in grado di fornire una velocità adeguata per l'ufficio, una buona autonomia e un funzionamento silenzioso. Tutto l'hardware trova posto in un leggero ed elegante chassis. Il display potrebbe però riprodurre i colori con maggior fedeltà.

Veloce con suite d'ufficio, lunga autonomia

SSD di piccola capienza

2 MEDION AKOYA E4251 (MD61561)

Prezzo: 340 Euro
http://bit.ly/maprezzo

Compatto e leggero, ma robusto. Chi cerca un notebook come si deve per la produttività, rimarrà soddisfatto dell'Akoya E4251: veloce con LibreOffice, silenzioso e con buona autonomia. Offre inoltre un buon set tastiera/touchpad. purtroppo in due ore e mezzo. Funziona in modo silenzioso.

+ Veloce con suite d'ufficio, buoni tastiera e touchpad

− RAM scarsa

3 MEDION AKOYA E4271 (MD61579)

Prezzo: 390 Euro
http://bit.ly/maprezzo2

Il Medion Akoya E4271 è l'unico notebook testato dotato di un touchscreen, che consente al dispositivo di essere utilizzato anche come tablet. La tecnologia a bordo è molto simile a quella offerta dal modello della stessa serie piazzatosi al secondo posto. Nella maggior parte delle prove ha ottenuto anche gli stessi voti.

Con touchscreen, buona combinazione tastiera/touchpad

RAM scarsa

RISULTATI DEL TEST

	ACER SWIFT 3	MEDION AKOYA E4251	MEDION AKOYA E4271
	Processore: Intel Pentium 4417U **Scheda grafica:** HD Graphics 610 **Display:** 14,0 pollici, 1.920 x 1.080 Pixel **Dimensioni:** 32,3 x 22,9 x 2,2 cm	**Processore:** Intel Pentium N5000 **Scheda grafica:** UHD Graphics 605 **Display:** 14,0 pollici, 1.920 x 1.080 Pixel **Dimensioni:** 32,9 x 22,0 x 2,0 cm	**Processore:** Intel Pentium N5000 **Scheda grafica:** UHD Graphics 605 **Display:** 14,0 pollici, 1.920 x 1.080 Pixel **Dimensioni:** 33,1 x 22,9 x 1,9 cm
Velocità di lavoro del notebook?	**Velocissimo con suite d'ufficio**	**Velocissimo con suite d'ufficio**	**Velocissimo con suite d'ufficio**
Velocità con applicazioni d'ufficio / elaborazioni video / accesso all'hard disk	veloce (48,5%) / un po' lento (37,5%) / veloce (51,9%)	veloce (48,8%) / un po' lento (35,9%) / un po' lento (44,3%)	veloce (48,5% / un po' lento (33,4%) / un po' lento (44,7%)
Velocità con i giochi (in DX11-/DX12): 1.366 x 768 Pixel / risoluzione nativa	molto scattosa (9 / 3 / 5 / 2 fps)	molto scattosa (7 / 2 / 4 / 1 fps)	molto scattosa (6 / 2 / 3 /2 fps)
Velocità USB: da SSD esterno a notebook / da notebook a SSD esterno	un po' lenta (256,0/ 222,6 MB/s)	un po' lenta (189,6/ 222,6 MB/s)	lenta (150,6 / 213,3 MB/s)
Qualità immagine e audio?	**Immagine come si deve**	**Scarsa fedeltà cromatica**	**Scarsa fedeltà cromatica**
Riproduzione cromatica (fedeltà), contrasto / distribuzione luminosità (scostamento max) / tempo di refresh (reattività)	molto bassa (55,1%) / molto elevato (100%) / uniforme (14,3%) / basso (14,35 ms)	molto bassa (55,1%) / molto elevato (100%) / uniforme (10,7%) / basso (14,22 ms)	molto bassa (55,1%) / molto elevato (100%) / uniforme (13,3%) / basso (12,88 ms)
Perdita luminosità nella visione laterale / Effetto antiriflesso	un po' elevata / intensi riflessi	elevata / intensi riflessi	elevata / intensi riflessi
Test visivo: qualità immagine su display integrato	elevata (colori pallidi)	molto elevata (colori pallidi)	elevata (colori pallidi)
Test visivo: qualità immagine su uscita digitale / analogica	molto elevata / manca	molto elevata / manca	molto elevata / manca
Qualità audio (Deviazione risposta in frequenza / Rumorosità / Distorsione)	ottima (0,14% / 95,12 db / 0,008%)	buona (0,13% / 79,49 dB / 0,021%)	buona (0,10% / 82,81 dB / 0,0010%)
Idoneità per un uso in mobilità?	**Oltre sette ore d'autonomia**	**Silenzioso, autonomia ok**	**Silenzioso, autonomia ok**
Autonomia (Produttività / visione film / durata ricarica)	lunga (7:10 / 6:14 / 2,22 h)	abb. lunga (5:26 / 4:51 / 3,54 h)	lunga (5:38 / 4:44 / 3,18 ore)
Rumorosità (Suite ufficio / Video / a pieno carico / con i giochi)	molto silenz. (0,2 / 0,1 / 0,6 / 0,4 Sone)	silenzioso	silenzioso
Quanto scalda dopo due ore: parte inferiore / retro	molto poco: 14,1 °C / 9,2 °C	molto poco: 14,6 °C / 10,2 °C	molto poco: 16,2 °C / 10.0 °C
Peso inclusa batteria / alimentatore con cavo	basso (1409 / 159 g)	molto basso (1338 / 182 g)	basso (1650 / 315 g)
La dotazione del dispositivo è completa?	**SSD piccolo**	**RAM scarsa**	**RAM scarsa**
Memoria di lavoro: integrata / espandibilità max.	scarsa: 4 / 20 (1 x 16) GB	scarsa: 4 GB / non possibile	scarsa: 4 GB / non possibile
Hard disk: Tipo / capienza / modello	SSD / 119 GB / Kingston RBUS-NS854P3128GJ	SSD / 238 GB / Phison S11.256G Phison-SSD B3	SSD / 238 GB / Phison S11-128G PHISON-SSD 83
Porte di Connessione	1 x USB 3.1 Tipo C, 2 USB 3,1 / 1 x USB 2.0, 1 x Headset, 1 x HDMI	1 x USB 3.1 Tipo C (con DisplayPort), 1 x USB 3.1, 1 x USB 2.0, 1 x Headset, 1 x Mini HDMI	2 x USB 3.1 Tipo C (con DisplayPort), 1 x USB 2.0, 1 x Headset
Standard WLAN /Frequenza WLAN / Bluetooth (Versione)	802.11ac /2,4 e 5 GHz/ 4.2	802.11ac /2,4 e 5 GHz/ 5	802.11ac /2,4 e 5 GHz/ 5
Possibilità di espansione	1 x DDR4	nessuna	nessuna
Card Reader (schede supportate) / Microfono / camera	si (SD) / si / si	si (micro SD) / si / si	si (microSD) / si / si
Programmi in dotazione	pochi	un po' pochi	pochi
Facilità d'uso?	**Tastiera e Touchpad buoni**	**Tastiera e Touchpad buoni**	**Unico con Touchscreen**
Qualità della tastiera / Qualità del touchpad	buona esperienza di scrittura, punto di pressione buono / superficie abbastanza ampia	buona esperienza di scrittura / abbastanza ampio, impossibile cliccare sul bordo superiore	tasti con buon punto di pressione / abbastanza ampio, impossibile cliccare sul bordo superiore
Usabilità del touchscreen	manca	manca	superficie un po' opaca
Ripristino del notebook alle impostazioni di fabbrica	Windows Recovery con restore dati	Windows Recovery con restore dati	Windows Recovery con restore dati
RISULTATO DEL TEST	**7**	**7**	**7**

4 HP 255 G7
(6BN37ES)
Prezzo: 512 Euro
http://bit.ly/h2prezzo

L'HP è il notebook più performante tra tutti quelli testati. Grazie al suo processore Ryzen offre una potenza che gli permette anche di eseguire montaggi video. L'HP si distingue, inoltre, per i giochi, sebbene riducendo la risoluzione (1.366 x 768 pixel), la riproduzione delle immagini rimane scattosa.

Elevata velocità di lavoro, RAM adeguata

Scarsa fedeltà cromatica

5 DELL INSPIRON 15
(3582-0J8V2)
Prezzo: 434 Euro
http://bit.ly/diprezzo

L'Inspiron è l'unico grande notebook (da 15 e 17 pollici) che lavora con estrema silenziosità. Offre una velocità adeguata per LibreOffice. La sua batteria consente un'autonomia di cinque ore e mezza, una durata decisamente più lunga rispetto ad altri candidati al test di grande formato.

Lunga autonomia, silenzioso

Scarsa fedeltà cromatica

6 TREKSTOR SURFBOOK
(A13B-PO)
Prezzo: 279 Euro
http://bit.ly/tsprezzo

Elegante, piccolo, leggero e con una potenza adeguata per gestire lavoro d'ufficio. Con il Surfbook di Trekstor si riesce a lavorare molto bene, ma offre una dotazione un po' misera: la RAM è di soli 4 Gigabyte. A bordo, anziché un SSD, monta una piccola e lenta memoria eMMC.

Leggero, silenzioso

Spazio di storage molto scarso

7 LENOVO V145-15
(81MT0016)
Prezzo: 380 Euro
http://bit.ly/lvprezzo

A bordo del Lenovo trova posto un processore AMD Athlon, che offre la stessa velocità dei Pentium della concorrenza. Con i giochi si rivela addirittura un po' più rapido, ma richiede un consumo di corrente più elevato. La batteria del V145-15 si esaurisce purtroppo in due ore e mezzo. Funziona in modo silenzioso.

RAM adeguata, ventole molto silenziose

Autonomia scarsa

8 ASUS VIVOBOOK 17
(F705MA-BX028T)
Prezzo: 450 Euro
http://bit.ly/avprezzo

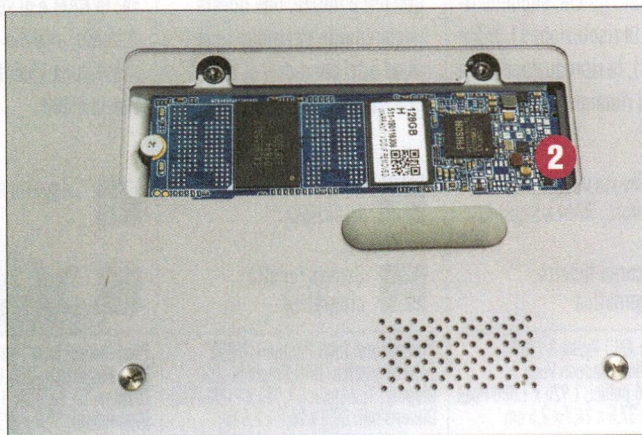
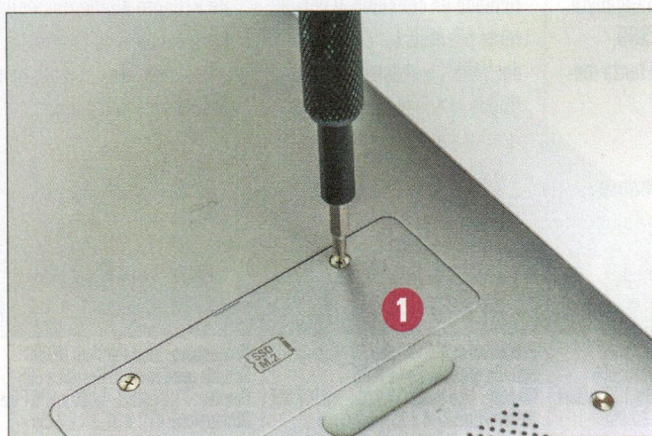
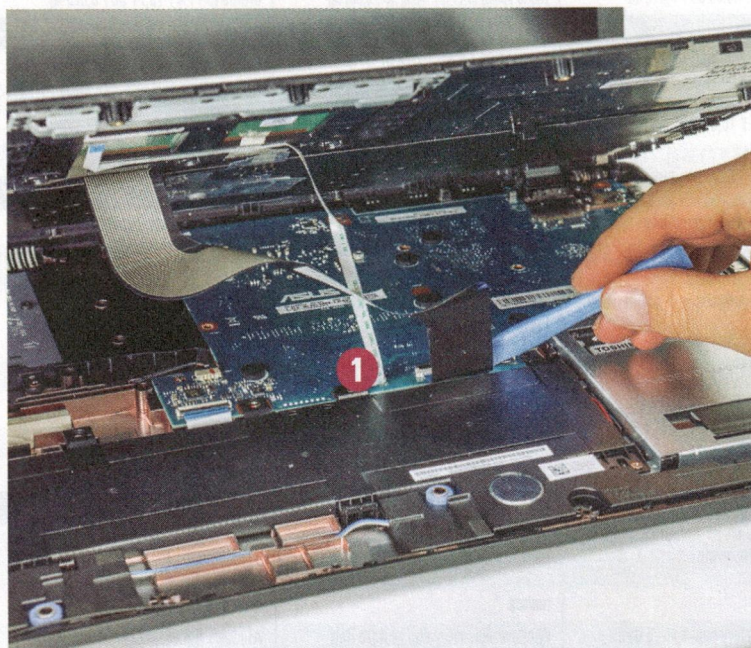
Il display del VivoBook è piuttosto ampio, ma più pixelloso di quelli della concorrenza. Lavorando con programmi d'ufficio, questo difetto infastidisce molto poco. Si rivela invece piuttosto irritante il rallentamento quasi del 50% della velocità di lavoro, causato dal lento hard disk a bordo dell'Asus.

+ Autonomia ok

− Velocità di lavoro mediocre

4 HP 255 G7	5 DELL INSPIRON 15	6 TREKSTOR SURFBOOK	7 LENOVO V145-15	8 ASUS VIVOBOOK 17
Processore: AMD Ryzen 3 2200U **Scheda grafica:** Radeon Vega 3 **Display:** 15,6 pollici, 1.920 x 1.080 Pixel **Dimensioni:** 37,5 x 24,7 x 2,6 cm	**Processore:** Intel Pentium N5000 **Scheda grafica:** UHD Graphics 605 **Display:** 15,6 pollici, 1.920 x 1.080 Pixel **Dimensioni:** 38,0 x 26,0 x 2,5 cm	**Processore:** Intel Pentium N5000 **Scheda grafica:** UHD Graphics 605 **Display:** 13,3 pollici, 1.920 x 1.080 Pixel **Dimensioni:** 31,5 x 21,1 x 2,1 cm	**Processore:** AMD Athlon A9-9425 **Scheda grafica:** Radeon R5 **Display:** 15,6 pollici, 1.920 x 1.080 Pixel **Dimensioni:** 37,6 x 25,4 x 2,6 cm	**Processore:** Intel Pentium N5000 **Scheda grafica:** UHD Graphics 605 **Display:** 17,0 pollici, 1.600 x 900 Pixel **Dimensioni:** 41,1 x 27,3 x 2,7 cm
Il più veloce del test	**Velocissimo con suite d'ufficio**	**Adeguato per suite d'ufficio**	**Adeguato per suite d'ufficio**	**L'hard disk rallenta la velocità**
veloce (62,3%) / un po' lento (42,8%) / veloce (47,74%)	veloce (45,5%) / un po' lento (34,4%) / un po' lento (43,3%)	un po' lento (40,1%) / un po' lento (30,3%) / un po' lento (31,3%)	un po' lento (41,2% / un po' lento (30,7%) / veloce (51,0%)	lento (23,5% / lento (27,9%) / molto lento (13,7%)
molto scattosa (18 / 6 / 9 / 3 fps)	molto scattosa (6 / 3 / 4 / 2 fps)	molto scattosa (4 / 1 / 3 / 1 fps)	molto scattosa (12 / 4 / 7 / 3 fps)	molto scattosa (6 / 2 /5/ 2 fps)
un po' lenta (365,7 / 124,9 MB/s)	un po' lenta (269,5 / 222,6 MB/s)	lenta (61,0 / 182,9 MB/s)	lenta (189,6 / 155,2 MB/s)	lenta (98,5/ 106,7 MB/s)
Refresh velocissimo	**Refresh velocissimo**	**Il miglior display del test**	**Angolo di visione limitato**	**Display un po' pixelloso**
molto bassa (55,1%) / molto elevato (95,4%) / poco uniforme (17,7%) / molto basso (4,65 ms)	molto bassa (55,10%) / molto elevato (98,80%) / uniforme (14,60%) / molto basso (4,58 ms)	elevata (87,40%) / molto elevato (100%) / poco uniforme (22,80%) / basso (13,58 ms)	molto bassa (56,00%) / elevato (92,10%) / poco uniforme (18,50%) / molto basso (4,70 ms)	elevata (94,80%) / molto elevato (100,00%) / uniforme (13,00%) / molto basso (5,77 ms)
molto elevata / rilascia riflessi minimi	molto elevata / rilascia minimi riflessi	elevata / rilascia riflessi	molto elevata / rilascia minimi riflessi	molto elevata / rilascia intensi riflessi
elevata (dipende molto dall'angolo di visione)	elevata (dipende molto dall'angolo di visione)	molto elevata (colori un po' pallidi)	elevata (dipende molto dall'angolo di visione)	elevata (dipende molto dall'angolo di visione)
molto elevata / manca	molto elevata / manca	molto elevata / manca	molto elevata / manca	molto elevata / manca
molto buona (0,11% / 93,70 dB / 0,008%)	buona (0,09% / 89,01 dB / 0,006%)	buona (0,14% / 80,60 dB / 0,016%)	molto buona (0,11% / 94,82 dB / 0,009%)	ottima (0,11% / 93,71 Db / 0,025%)
Autonomia ok	**Silenzioso, autonomia ok**	**Silenzioso, leggero**	**Autonomia scarsa**	**Non si scalda**
abb. lunga (3:45 / 3:13 / 2,13 h)	lunga (5:29 / 4:29 / 2,42 h)	abb. lunga (3:16 / 3:15 / 3,17 h)	breve (2,30 / 1:54 / 2,16 h)	abb. lunga (4:42 / 4:19 / 2:15 h)
silenzioso (0,3 / 0,3 / 1,4 / 1,1 Sone)	silenzioso	silenzioso	molto silenz. (0,1 / 0,1 / 0,3 / 0,3 Sone)	silenzioso (0,2 / 0,3 / 1,0 / 1,0 Sone)
pochissimo: 15,6 °C / 13,6 °C	poco: 22,0 °C / 7,6 °C	poco: 21,0 °C / 10,8 °C	molto poco: 13,9 °C / 12,1 °C	molto poco: 9,1 °C / 5,9 °C
basso (1924 / 275 g)	basso (1888 / 266 g)	molto basso (1229 / 138 g)	basso (1956 / 175 g)	basso (2163 / 129 g)
Offre RAM adeguata	**Lavora veloc. anche senza SSD**	**RAM scarsa**	**RAM adeguata**	**RAM scarsa**
un po' scarsa: 8 / 32 (2 x 16) GB	scarsa: 4 / 8 GB (1 x 8) GB	scarsa: 4 GB / non espandibile	un po' scarsa: 8 / 16 (1 x 16) GB	scarsa: 4 GB / non espandibile
SSD / 238 GB / Micron MTFD DAV256TBN-1AR1ZABHA	SSD / 238 GB / SK Hymix BC501 NVMe	eMMC / 58 GB / Generic SLD6462	SSD / 238 GB Samsung MZ7LN-256HAlq-000L2	Hard disk / 931 GB / Toshiba MQ04BF100
2 USB 3.1, 1 x USB 2,0, 1 x Headset, 1 x HDMI, 1 x porta Ethernet (1000 Mbit)	2 USB 3.1, 1 x USB 2.0, x Headset, 1 x HDMI	2 x USB 3.1, 1 x Headset, 1 x Mini HDMI	2 x USB 3.1, 1 x Headset, 1 x HDMI, 1 x Porta Ethernet (1000 Mbit)	1 x USB 3,1 Tipo C, 1 x USB 3.1, 2 x USB 2.0, 1 x Headset, 1 x HDMI, 1 x Porta Ethernet (1000 Mbit)
802.11ac / 2,4 e 5 GHz / 4.2	802.11ac / 2,4 e 5 GHz / 5	802.11ac / 2,4 GHz / 4.2	802.11ac / 2,4 Ghz e 5 GHz / 4,2	802.11ac / 2,4 GHz e 5 GHz / 5
1 x DDR4	1 x hard disk 2,5 pollici	1 x M.2 SATA	nessuna	nessuna
si (scheda SD) / si / si	si (SD, MMC) / si / si	si (microSD) / si / si	si (scheda SD, MMC) / si / si	si (scheda SD, MMC) si / si
un po' pochi	un po' pochi	un po' pochi	un po' pochi	un po' pochi
Tastiera e Touchpad ok	**Tastiera e Touchpad ok**	**Tastiera e Touchpad ok**	**Tastiera e Touchpad ok**	**Tastiera e Touchpad ok**
tasti un po' ruvidi / semplice da usare, con tasti dedicati	layout un po' compresso / superficie un po' ruvida, gestibile abbastanza bene	layout tastiera un po' insolito / superficie touchpad confortevole	tasti con punto di pressione abbastanza buono / superficie liscia del touchpad	layout tasti un po' compresso / un po' piccolo per un modello da 17 pollici
manca	manca	manca	manca	manca
Windows Recovery con restore dati	Windows Recovery con restore dati	Windows Recovery con restore dati	Windows Recovery con restore dati	Windows Recovery con restore dati
7	**6**	**6**	**6**	**6**

Potenzia il tuo Notebook

PIÙ MEMORIA: UN SSD PIÙ CAPIENTE

Se è presente **un coperchio** ❶ per eseguire la manutenzione, come offerto dai due notebook di Medion, potenziare il dispositivo sarà un gioco da ragazzi. Dopo aver rimosso una o due viti sarà possibile asportare il coperchio. Dietro al coperchio trova posto l'**SSD** ❷ che generalmente presenta il formato 22 x 80 millimetri, poiché solo pochi produttori installano modelli di SSD più piccoli (22 x 42 millimetri), come offerto dal Trekstor. Dopo aver tolto la vite di ritegno, sarà possibile rimuovere agevolmente l'SSD, per sostituirlo con un esemplare di maggior capienza. Attenzione: entrambi gli SSD devono presentare le stesse caratteristiche tecniche. Le specifiche tecniche del notebook riportano se deve essere un modello con interfaccia SATA (di prezzo più economico - 500 GB a partire da 60 Euro su **http://bit.ly/ssd500m2**) o di un esemplare PCIe (più veloce, 500 GB a partire da 100 Euro su **http://bit.ly/ssd500pcie**).

PIÙ VELOCITÀ: SOSTITUZIONE DELL'HARD DISK

A bordo del notebook di Asus trova posto un **hard disk tradizionale.** Grazie alla sua capienza di 1.000 Gigabyte offre più spazio di storage, ma si rivela piuttosto lento. Ottimo che sia possibile sostituirlo con un SSD nel formato da 2,5 pollici (500 GB a partire da 60 Euro su **http://bit.ly/ssd500gb**), per ottenere un consistente aumento della velocità di lavoro. L'apertura dello chassis dovrà essere eseguita con una certa delicatezza. Dopo avere allentato le viti nella parte inferiore, bisognerà sollevare il coperchio della tastiera, ribaltandolo con un'angolazione di circa 30 gradi, senza staccare il cavo ❶ per la tastiera e il mouse. Le viti della cornice dell'hard disk potranno essere allentate più agevolmente, utilizzando un cacciavite a stella.

PIÙ PERFORMANTE: ESPANSIONE DELLA RAM

Con i notebook economici, i produttori sono ben lieti di risparmiare sulla **memoria di lavoro (RAM)**. Solo due modelli tra i notebook testati offrono una RAM da 8 Gigabyte, tutti gli altri sono equipaggiati con una memoria di soli 4 Gigabyte. Espandere la RAM (di tipo SODIMM) è comunque piuttosto semplice: sul notebook di Dell, il socket per la RAM trova posto, ad esempio, direttamente sotto la piastra della base. La sostituzione avviene in modo semplice: spegnere il notebook, svitare la piastra e procedere a inserire il nuovo modulo ❶. 8 Gigabyte di RAM costano circa 35 Euro su **http://bit.ly/8gbramsodimm**.

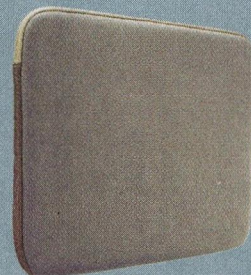
AL POSTO DEL PC: UTILIZZO DEL NOTEBOOK COME DESKTOP

Attraverso un monitor (è sufficiente un modello da 24 pollici Full-HD da 100 Euro su **http://bit.ly/nuovomonitor24**) ed un set tastiera/mouse (come il Logitech MK270 che trovi su **http://bit.ly/kittmlogi**) sarà possibile utilizzare un notebook come PC Desktop. Ad esempio, si potrà visualizzare il programma di eMail sul display del notebook, mentre si utilizzerà il monitor per giocare o per continuare a lavorare.

ACCESSORI PER IL VOSTRO NOTEBOOK

Mouse per notebook
Chi preferisce utilizzare un mouse anche in mobilità, potrà scegliere un modello ad hoc per i notebook (10 Euro su **http://bit.ly/mousesenzafili**), che troverà posto in qualsiasi tasca.

Pendrive USB
Tramite una pendrive USB 3.1 è possibile trasferire velocemente grandi quantitativi di dati. Il modello da 256 GB che trovi su **http://bit.ly/pendrive31256** costa circa 45 Euro.

Borsa per notebook
Se parti per un viaggio, conviene acquistare una borsa imbottita per trasportare il notebook (a partire da 15 Euro su **http://bit.ly/borsanotebook**), che offrirà anche spazio per contenere altri accessori.

Custodia per notebook
Se non si vuole una borsa si potrà infilare il notebook in una custodia imbottita (a partire da 8 Euro su **http://bit.ly/custorianotebook**

Windows? Fuori dalla finestra!

Chi compra un PC ha il diritto di rinunciare al software preinstallato, ottenendo un rimborso... ma nella realtà, le cose non sono così semplici

L'acquisto di un nuovo PC si presenta sempre con un classico problema: il costo della licenza di Windows. Quasi tutti i computer vengono infatti venduti con Microsoft Windows preinstallato, e ovviamente questo ha comunque un costo. Nell'ormai lontano 2014 la Corte di Cassazione italiana ha stabilito che, se l'utente utilizza la clausola di rinuncia prevista dal contratto di Microsoft (EULA), si ha diritto a ricevere il rimborso del prezzo della licenza non utilizzata. Al primo avvio del sistema operativo è infatti necessario accettare la licenza: se non lo si fa, formattando subito il computer, la licenza di Windows non è stata utilizzata, e ne consegue che si ha diritto a ricevere il rimborso del prezzo pagato. Nel contratto di Windows 10 (***http://bit.ly/windowscontratto***) è infatti presente la frase:

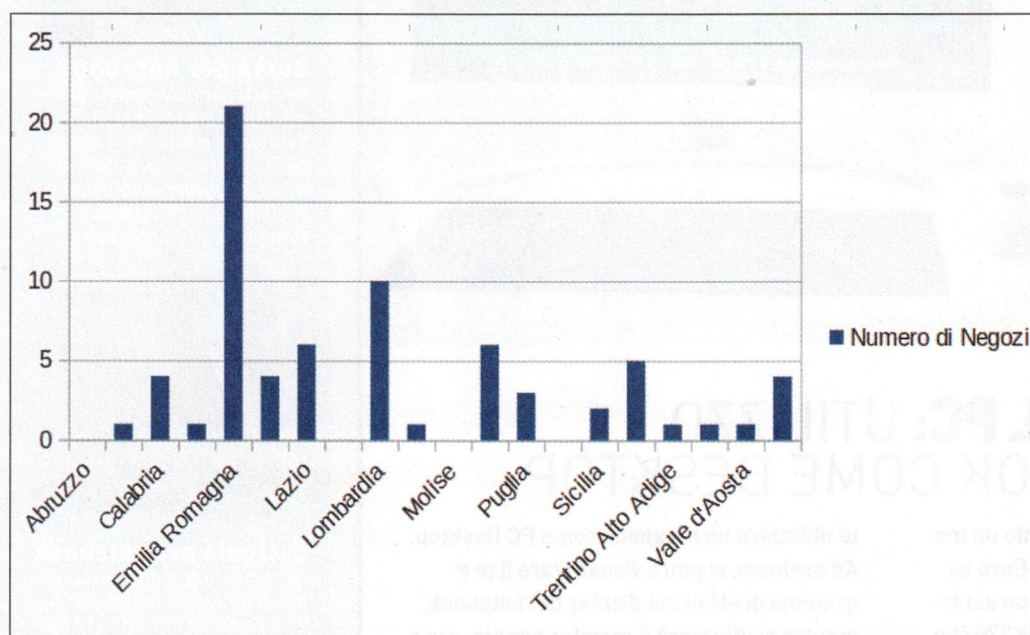
Qualora il licenziatario non accetti le presenti condizioni e non vi si conformi, non potrà utilizzare il software né le relative funzionalità. Il licenziatario potrà contattare il produttore del dispositivo o l'installatore oppure il rivenditore, qualora abbia acquistato il software direttamente, per conoscere le modalità di restituzione del software o del dispositivo e di rimborso del prezzo.

Al momento non esiste una legislazione europea su questo tema: il 7 settembre 2016 la corte di giustizia europea ha stabilito soltanto che non è espressamente illegale vendere hardware e software assieme. Ciò significa che i computer possono ancora essere venduti con un sistema operativo a pagamento di serie, ma per quanto riguarda il rimborso in caso di rinuncia all'acquisto del software bisogna rifarsi proprio alla sentenza della Cassazione. Sentenza che recita:

[...]chi acquista un computer sul quale sia stato preinstallato dal produttore un determinato software di funzionamento (sistema operativo) ha il diritto, qualora non intenda accettare le condizioni della licenza d'uso del software propostegli al primo avvio del computer, di trattenere quest'ultimo restituendo il solo software oggetto della licenza non accettata, a fronte del rimborso della parte di prezzo ad esso specificamente riferibile.

Per la legge italiana la logica è semplice: se si acquistano hardware e software e si vuole rinunciare solo al software, è giusto ricevere il rimborso per il programma non utilizzato.

LA SITUAZIONE REALE

Nella realtà però è molto difficile ottenere un rimborso. Al momento solo Acer offre un link sul proprio sito con le istruzioni per il rimborso dell'OS non utilizzato (***http://bit.ly/rimborsoacer***), e Asus offre il rimborso dopo aver contattato l'assistenza via email (***info@asus.it***). Per gli altri produttori non ci risulta che gli utenti abbiano avuto fortuna con le loro richieste di rimborso. L'unica soluzione sarebbe procedere in tribunale, facendo valere la sentenza della Corte di Cassazione n.19161 del 2014. Ma è ovvio che non convenga farlo, visto che il costo di una licenza di Windows è decisamente inferiore alle spese legali che si dovrebbero sostenere.
Una buona soluzione pratica consiste nell'acquistare i propri dispositivi in un negozio dichiaratamente GNU/Linux friendly: si può trovare quello più vicino a casa propria visitando l'indirizzo ***http://bit.ly/linuxsi***

Secondo LinuxSi, in cui i negozi Linux-friendly possono segnalare la propria presenza, esistono posti in cui comprare computer dotati di GNU/Linux nella maggioranza delle regioni

Tips & Tricks

Trucchi e consigli per usare subito GNU/Linux da vero esperto. Scoprire le strategie e gli strumenti giusti per trovare una soluzione rapida a tutti i problemi e sfruttare appieno le potenzialità del sistema e delle applicazioni

LEGENDA

- DATABASE
- GIOCHI
- GRAFICA
- HARDWARE
- KERNEL
- MULTIMEDIA
- RETE
- SHELL
- SICUREZZA
- SISTEMA
- SVILUPPO

BROWSER LEGGERI

Oggigiorno sembra che la guerra dei browser si sia un po' placata. Ogni browser Web pare aver trovato il proprio "equilibrio" e la propria direzione di sviluppo così come ogni utente pare abbia fatto la scelta su quale debba essere il browser predefinito da utilizzare con la propria distribuzione. Distratti da questa diatriba su quale sia il migliore in termini di performance, minore risorse utilizzate, aderenza agli standard ecc si è perso un po' di vista lo sviluppo di browser per così dire "secondari" che fanno della leggerezza e personalizzazione – o altri paradigmi – il proprio cavallo di battaglia cercando al tempo stesso di avere un motore di rendering che non dia problemi con nessuna pagina Web e con una interfaccia grafica intuitiva da utilizzare. Con queste premesse non possiamo non nominare due browser. Il primo è **Pale Moon** (***http://bit.ly/orgpalemoon***) - un fork datato 2009 del browser Firefox – il cui target di sviluppo vede velocità, leggerezza e personalizzazione tanto da coniarne il motto, che campeggia sul sito del progetto, **your browser, your way** (il tuo browser, come lo vuoi tu). Al momento di scrivere è arrivato alla versione **28.8.1** e per l'installazione è possibile adottare i pacchetti presenti nei repository della propria distribuzione e, se datati, optare per il file **palemoon-28.8.1.linux-x86_64.tar.xz** (scaricabile dal sito del progetto), decomprimerlo e lanciare l'eseguibile **palemoon**. Il motore di rendering non è il noto **Gecko** (***http://bit.ly/devgecko***) che equipaggia Firefox bensì un suo fork di nome **Goanna** (***http://bit.ly/moonchildpgoanna***). La pagina di default personalizzabile è in collaborazione con **start.me** (***https://start.me***) così come il motore di ricerca predefinito è **DuckDuckGo** mettendo così da parte i colossi **Yahoo** e **Google** che comunque rimangono selezionabili, a discrezione dell'utente. Diversi gli add-on che è possibile aggiungere: dalle estensioni (sviluppo Web, utility varie, gestione download) ai temi, dai plugin ai pacchetti per la localizzazione (se installato tramite gestore dei pacchetti della distribuzione quest'ultimo passaggio è automatico a meno di provvedere diversamente manualmente). Con lo stesso motore di rendering e derivato sempre da Firefox abbiamo il secondo browser, **Basilisk** (***http://bit.ly/basiliskbrowser***) sviluppato dallo stesso creatore di **Pale Moon** ma con un diverso paradigma. Trattasi infatti di un progetto **perpetual beta**, ovvero non c'è alcuna distinzione tra rilascio stabile e di sviluppo. In sostanza ad ogni correzione di bug è possibile scaricare la nuova versione nella quale non è da escludere la presenza di funzioni aggiuntive che gli utenti stessi dovranno eventualmente testare, e riferire di possibili malfunzionamenti/bug affinché possano essere corretti e rilasciare così una nuova versione.

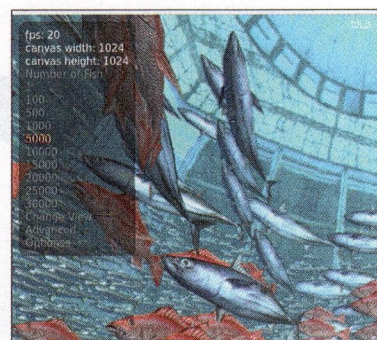



Fig. 2 • Basilisk durante i test sulle WebGL (www.khronos.org/webgl/)

Per entrambi i browser 1GB di RAM (al limite 2GB se si ha la tendenza ad aprire decine di tab quando si naviga) sono più sufficienti pertanto la loro installazione è suggerita su macchine datate. Tipicamente, ma non esclusivamente, portatili, così come su PC desktop performanti qualora si vogliano destinare le risorse verso altre applicazioni e non verso un browser.

Nelle figure 1 e 2 possiamo vedere i due browser alle prese con alcuni test tipici che è possibile attuare in questi casi. Generalmente i test – con i quali è possibile confrontare il browser preferito con i due suggeriti – sono il classico **Acid Test** (***http://bit.ly/sitoacidtests***) per l'aderenza agli

Fig. 1 • PaleMoon 28.8.1 e il risultato del test HTML5

standard **CSS** (**Cascading Style Sheets**), **HTML5Test** (***https://html5test.com***) per HTML5, **BrowserBench** (***https://browserbench.org***) per il test su javascript, performance grafiche e reattività del browser. Infine, anche se strettamente dipendente dai driver della scheda grafica, segnaliamo la verifica al supporto alle **WebGL** (***https://get.webgl.org/***) e in caso positivo l'esecuzione dei test associati ***http://bit.ly/webglsamplesgit***.

AUMENTARE LA DURATA DELLE BATTERIE

Powertop (https://01.org/powertop/) è una utility inizialmente sviluppata da Intel che permette di conoscere il carico di lavoro della CPU – e di ogni suo singolo core in presenza di CPU multicore come oggi è la norma – contando il numero di volte che la stessa CPU viene richiamata dai vari processi, e per quanto tempo i suddetti processi rimangono attivi facendo così uscire la CPU dal suo stato **idle**. L'utility è praticamente presente nei repository di tutte e distribuzioni quindi la sua installazione può risolversi utilizzando il gestore dei pacchetti (e.g. **sudo apt-get install powertop** su Debian e derivate). Una volta installato **Powertop** necessita di accedere all'hardware della macchina per effettuare le dovute misure e in quanto tale occorre lanciarlo con i privilegi dell'amministratore, e.g. **sudo powertop** o lanciarlo da utente **root**. In questo modo visualizzerà nella shell diversi rapporti associati ad analoghi menù nei quali ci si sposta con il tasto **Tab**. Interessante la sezione **Tunables** nella quale con l'aggettivo **Bad** si indicano configurazioni non ottimizzate, mentre con **Good** le configurazioni che fanno risparmiare energia e che sono attive nella macchina. Nel tab **Idle stats** è possibile vedere la percentuale del tempo della CPU nel **C-State** o **C-Mode** (Figura 3).

Occorre sapere che ogni CPU dispone di diverse modalità di funzionamento indicate con la lettera **C** seguita da un numero: più alto è il numero più la CPU è inattiva. Nel senso che disabilita un certo numero via via crescente di funzioni che così permettono di ridurre i consumi. Lo stato **C0** (**Operating State**) identifica la modalità attiva. Nello stato **C1** (**Halt**) le temporizzazioni interne principali della CPU sono interrotte via software mentre i bus dell'interfaccia e l'**APIC** (**Advanced Programmable Interrupt Controller**) funzionano alla loro piena velocità (ovvero frequenza). Lo stato **C2** (**Stop Grant**) vede le temporizzazioni principali della CPU interrotte in hardware mentre bus e APIC sono sempre attivi. Ad ogni incremento di numero viene spenta qualche funzione fino ad arrivare allo stato **C6** (**Deep Power Down**) nel quale viene ridotta anche a 0 la tensione interna della CPU. Esistono, inoltre, dei **"sotto-stati"** C come **C1E** (**Enhanced Halt**) che interrompe tutte le temporizzazioni principali della CPU e in più inizia gradatamente a ridurre le tensioni interne alla CPU mentre bus e APIC viaggiano sempre a piena velocità. Da quanto detto è evidente come sia possibile regolare in maniera granulare il risparmio energetico agendo su diversi stati della CPU (ma non solo). Tale utility allora si dimostra particolarmente indicata per i portatili poiché le ottimizzazioni portano ad un sensibile miglioramento della durata della batteria. Per tale motivo è suggerito lanciare **powertop** da un portatile **alimentato solo a batteria** e, ancora meglio, fargli generare un report utilizzando il comando **powertop --html** (anteponendo **sudo** qualora non si abbiano i privilegi dell'amministratore). Il comando genererà un report in html nella cartella dove è stato lanciato, report che possiamo aprire con un browser per le consultazioni (Figura 4) e laddove nel tab **Tuning** è possibile analizzare le possibili ottimizzazioni da mettere in atto.

Un'osservazione sulla specifica **VM writeback timeout** il cui valore suggerito è **1500** centesimi di secondo (15 secondi) in luogo del valore di default 500 centesimi di secondo (5 secondi) come è facile verificare con il comando **cat /proc/sys/vm/dirty_writeback_centisecs**. Questa opzione aumenta da 5 a 15 secondi i **kernel flusher** ovvero i thread utilizzati dal kernel per scrivere i dati su disco. Questo vuol dire che – in linea di principio – se dovesse venir meno la corrente di alimentazione si possono perdere al più gli ultimi 15 secondi di dati. Se il pericolo è più reale per un desktop, a meno di avere un **UPS** (**Uninterruptible Power Supply**) collegato, lo è molto meno per i portatili in primo luogo perché in caso di mancanza della corrente interverrebbe l'alimentazione a batteria e in secondo luogo anche in assenza di alimentazione da rete e presenza di batterie scariche il sistema software avviserebbe del livello di scarica permettendo così di salvare il lavoro e/o iniziare – laddove possibile – la fase di ricarica delle batterie. Dal sito del progetto è possibile scaricare il manuale in pdf per approfondimenti d'uso.

```
~ : powertop — Konsole
File  Modifica  Visualizza  Segnalibri  Impostazioni  Aiuto
PowerTOP v2.10   Overview   Idle stats   Frequency stats   Device stats   T

           Pkg(OS)  |            CPU(OS) 0
POLL        0,0%    | POLL        0,0%    0,0 ms
C1          2,1%    | C1          4,4%    0,2 ms
C2         94,3%    | C2         90,9%    1,4 ms

                    |            CPU(OS) 1
                    | POLL        0,0%    0,0 ms
                    | C1          0,1%    0,1 ms
                    | C2         96,5%    3,4 ms
```

Fig. 3 • A sinistra la percentuale in stato C, a destra il report su ogni core

Fig. 4 • Le ottimizzazioni suggerite da Powertop

Intrappolati in un cerchio magico

■ **Pronti per una storia intelligente e divertente? Basta provare il titolo che ci apprestiamo a riportare, disponibile su Steam**

The Magic Circle v. 4114

Licenza: Free Demo
Sito Web: http://bit.ly/magiccirclegame
Tipo: Gioco

Sviluppato e pubblicato dalla piccola software house **Question** (***http://bit.ly/questiongames***), basato sull'onnipresente motore grafico **Unity** (***http://bit.ly/unitygamedev***) e rilasciato nel Luglio del 2015, **The Magic Circle** è un gioco un po' fuori dal comune: rientra nel genere **sandbox** con unica modalità di gioco in **single player**. I **sandbox game** sono titoli caratterizzati da una particolarità: il giocatore ha la capacità di realizzare e quindi continuare e terminare il gioco stesso distruggendo e/o modificando gli oggetti dell'ambiente nel quale è immerso. Anticipiamo che il gioco è localizzato in Italiano – anche nella versione demo – solo nei sottotitoli mentre le voci sono tutte in Inglese.

COME SI INSTALLA?

Non c'è scelta, se vogliamo iniziare a provare il gioco nella versione demo – per poi deciderne l'acquisto – l'unica strada è installare il client Steam sebbene ci sia da dire che da un po' di tempo sono in fase di sviluppo alcune piattaforme open source che pare possano sostituire il client Steam. In che modo e con quali compatibilità lo verificheremo nei prossimi numeri su questa stessa rubrica provandole con l'installazione di un titolo. Premesso questo ricordiamo – soprattutto a chi si avvicina al mondo GNU/Linux – che l'installazione del client di **Valve Corporation** (***http://bit.ly/valveit***) è per così dire "indiretto". Infatti il pacchetto presente nei repository delle distribuzioni contiene l'installer del client. In sostanza una volta installato il pacchetto – tipicamente di nome **steam-<numero_versione>** - con il gestore dei pacchetti della distribuzione in uso, occorre trovare e lanciare dal menù generale la voce **Steam** che avvia l'installer il quale a sua volta scarica e installa in automatico il client e come ultimo passo associa la voce **Steam** del menù al client e non più all'installer. Nel frattempo durante il download occorre creare un **account steam** dal sito ufficiale ***http://bit.ly/steampow*** e le cui credenziali inserite dovranno poi essere utilizzate per accedere con il client e passare così all'installazione del gioco che avviene cliccando sul menù **STORE**, digitando **The Magic Circle** nel rigo di ricerca e optando per **The Magic Circle Demo – Free Demo**. Nella nuova pagina cliccare sul pulsante verde **Play Game** per far partire l'installazione del gioco.

Il client Steam è in genere localizzato in Inglese. Per cambiare i menù e tutte le voci in Italiano è sufficiente cliccare in alto a sinistra sul menù **Steam** e optare per **Settings**. Nella nuova pop-up dal gruppo di voci di sinistra cliccare su **Interface** e nel primo menù a tendina in alto selezionare **Italiano** cliccare su **OK** e riavviare il client. A questo punto possiamo lancia-

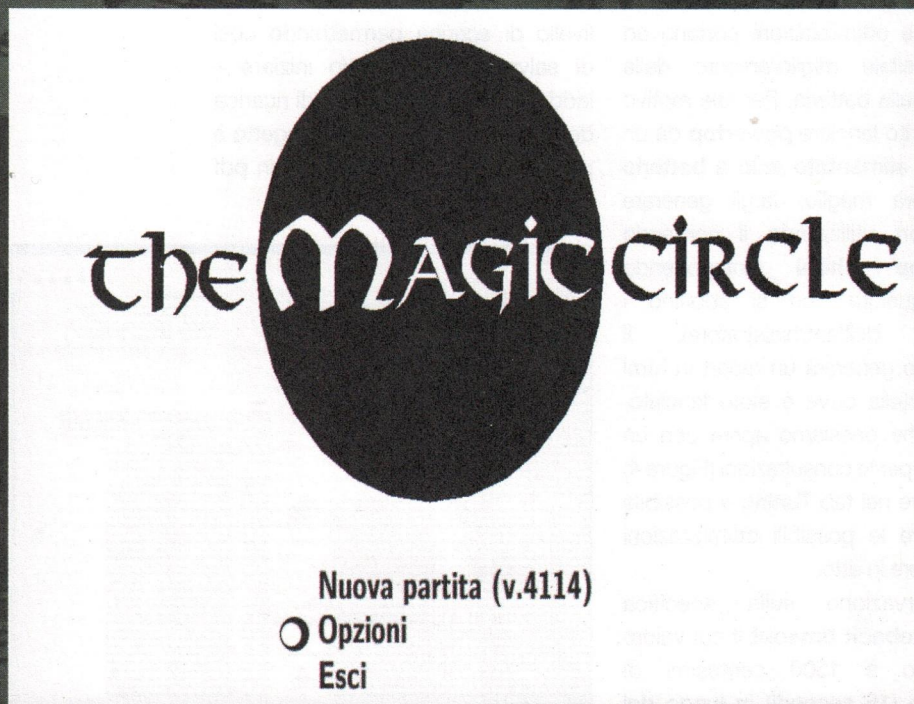



Fig. 1 • Sembra che anche il menù generale sia da completare...

re il gioco dal client Steam andando nel menù **Libreria** optando per **Pagina iniziale** e, nella nuova schermata, cliccare sul tasto play recante il nome del gioco.

DA FANTASCIENZA AD AVVENTURA

Si immagini di essere in un fumetto creato da un disegnatore il quale non lo ha terminato in tutte le parti: alcuni oggetti – come promemoria – sono solo abbozzati con forme e funzioni bizzarre. Ora si immagini di entrare in quel fumetto che nel frattempo è stato trasformato in videogioco e di essere proiettati fisicamente in piccolo all'interno di esso. Questo è lo scenario da immaginare nel momento in cui lanceremo il gioco nel quale si alterneranno scherzi, momenti di enigmistica intelligente e divertente alternati a situazioni grottesche o pericolose.
Ad esempio dopo aver seguito tutti e tre i tutorial e proseguendo il cammino ci ritroveremo ad essere attaccati da una sorta di "cane urlatore". Orbene dovremo intrappolarlo prima che ci ammazzi e solo dopo sarà possibile cambiarne il comportamento facendo in modo che ci veda come un soggetto amico e non nemico. Sarà così possibile "addestrarlo" affinché attacchi i nostri nemici così come sarà possibile "svuotarlo" delle sue caratteristiche per poi assegnarle ad altri. L'editing delle creature implicala la scelta di un certo numero di parametri, una sorta di programmazione utilizzando parole all'interno di un elenco: la dinamica ricorda un po' software come **Snap!** (*https://snap.berkeley.edu/*) e **Scratch** (*https://scratch.mit.edu/*). Tutte le creature "nostre amiche" ci seguiranno lungo il percorso. Ma abbiamo svelato fin troppo rischiando di togliere il gusto di giocare. Ora tocca a voi capire come superare tutti gli ostacoli, risolvere di volta in volta gli enigmi e sconfiggere i nemici.

LE SPECIFICHE DEL COMPUTER

Bianco e nero ma anche colori

Con una grafica che ricorda molto i fumetti in bianco e nero The Magic Circle non è un titolo avido di risorse pertanto molti utenti, se spinti dalla curiosità, potranno provarlo senza alcun problema se hanno una macchina con almeno un processore AMD Athlon 2,4GHz o equivalente Intel, 2GB di memoria RAM (meglio 4GB considerando l'ambiente desktop nel quale dovrà essere lanciato), una scheda video con almeno 512MB di RAM video a partire da una GeForce 8800 o equivalente ATI (e.g. Radeon HD 4830) o che comunque supportino le **Shader Model 4.0** (quindi tutte le schede grafiche a partire dal 2008 vanno bene). Infine occorre circa 1GB di spazio su hard disk per la versione demo: coloro che passeranno alla versione full necessiteranno di almeno 2GB.

Impostazioni iniziali

Italiano, miscelazione audio e comandi

Opzioni
Base
Avanzate
Gioco
Video
Audio
Comandi
Qualità illuminazione 100
Distanza ombre 50.0
V-Sync
Filtri anisotropici
Qualità shader Migliorata
Qualità texture Normale
Qualità ombre Alta
Applica
Annulla
Predefinite

Assegnazione tasti
Muoviti avanti W
Muoviti a sinistra A
Muoviti indietro S
Muoviti a destra D
Salta Barra spaziatrice
Usa F
Zoom MAIUSC sinistro
Raccogli/Lancia F
Mappa M
Riempi
Drain
Evoca alleati Nessuna (Tieni premuto Fill+Drain)
Modifica E
Obiettivo alleato Q
Inventario I
Cambia equipaggiamento Tab (Rotellina del mouse)
Seleziona trappola 1
Seleziona destinazione 2
Indietro
Predefinite

01 LOCALIZZAZIONE

Come anticipato la versione demo implementa i sottotitoli e menù in Italiano, ma occorre attivarli. Al primo lancio dal menù generale click su **Options** quindi andiamo nella sezione **Audio**, spuntiamo la casella **Subtitles** e a fianco nel menù **Language** scegliamo **Italiano**. La commutazione sarà automatica senza necessità di riavvio.

02 AUDIO E VIDEO

Sempre in **Audio** possiamo miscelare i livelli della musica degli effetti ecc con gli slider in alto se quelli di default (tutti al 100%) non sono di nostro gradimento. Spostiamoci in **Video**: ci vengono propinati due tab. Regoliamo i parametri in base alla potenza del nostro PC e del tipo di scheda grafica.

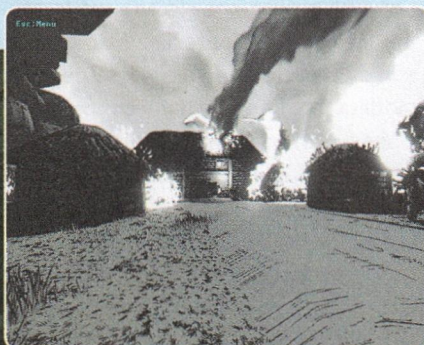
03 TASTIERA E MOUSE

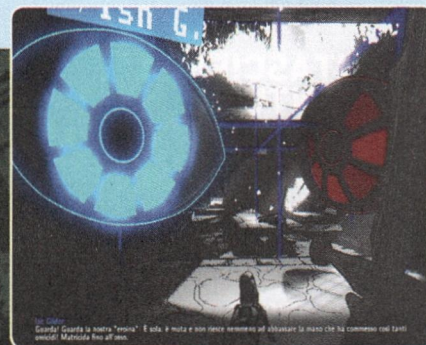
A questo punto andiamo in **Comandi**. Se non abbiamo un gamepad l'omonimo tab non ci interessa pertanto in **Tastiera/mouse** click su **Assegnazione** tasti per memorizzare le funzioni dei tasti di gioco. Prima di ritornare al menù ricordiamoci di cliccare su **Applica** altrimenti perderemo tutta la configurazione fin qui realizzata.

I primi suggerimenti

Familiarizziamo con l'ambiente di gioco

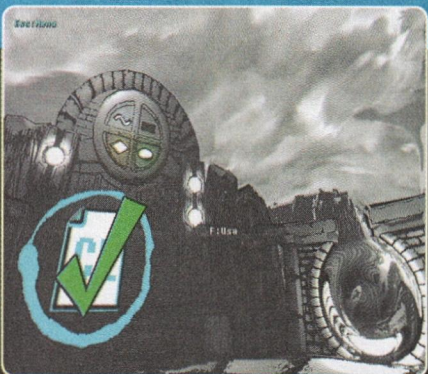
01 SI GIOCA

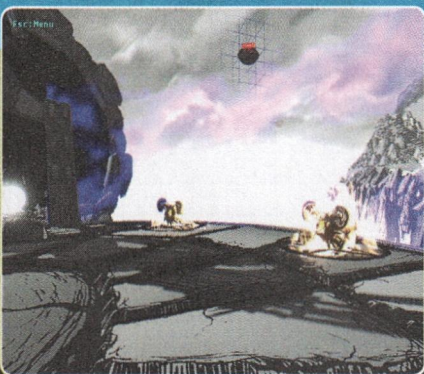
Ritornati al menù generale non ci resta che iniziare una partita cliccando sull'omonima voce. Partirà un divertente video introduttivo sottotitolato in Italiano. È possibile saltare la parte introduttiva premendo **Esc**, come d'altronde suggerito in maniera scherzosa da una delle voci narranti.

02 PRIMO PASSO

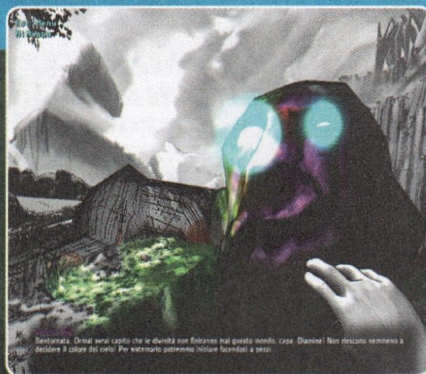
Al termine del video potremo iniziare a giocare. Il tutto ha inizio all'interno di una capanna illuminata da una lampada ondeggiante a causa del vento. Dirigiamoci verso la porta e quando siamo in prossimità di essa pigiamo il tasto F per aprirla. Di volta in volta appariranno a schermo i suggerimenti.

03 IL VILLAGGIO

Usciti dalla capanna, l'ambiente - in perfetto stile fumettistico - è quello di un villaggio che va a fuoco (immagine precedente). Giriamo un po' e bussiamo alle capanne dopodiché andiamo in fondo al capannone presente alla fine della strada e facciamoci consegnare la spada. Inizierà la prima discussione tra gli sviluppatori.

Dispute e magie

Discussioni tra sviluppatori e "strani fenomeni"

01 GLI OGGETTI

Usciamo dal capannone dalla parte opposta da dove siamo entrati girando subito a destra e di nuovo interverranno gli sviluppatori ma in questo caso possiamo camminare fino in fondo dove avremo un **Changelog** ologramma da leggere (tasto **F**). Recuperiamo gli oggetti dalle 4 sfere tremolanti e lanciamoli verso l'alto ad incastrarsi sopra la porta.

02 SIAMO FANTASMI

Aperta la porta andiamo verso l'alto fino dove gli sviluppatori stanno discutendo: verremo intrappolati, uccisi e diventeremo un fantasma e, in quanto tali, potremo interagire con tutti gli oggetti. A questo punto andiamo avanti e dirigiamoci verso la "luce"... per ritornare di nuovo al menù principale.

03 SI RIPARTE!

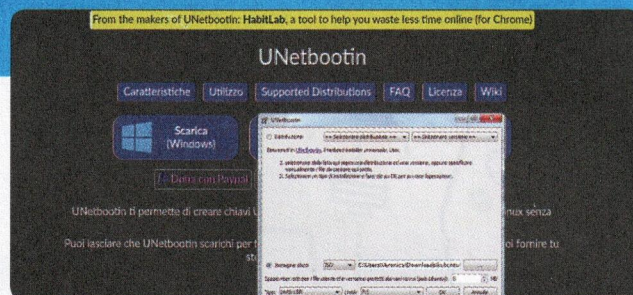
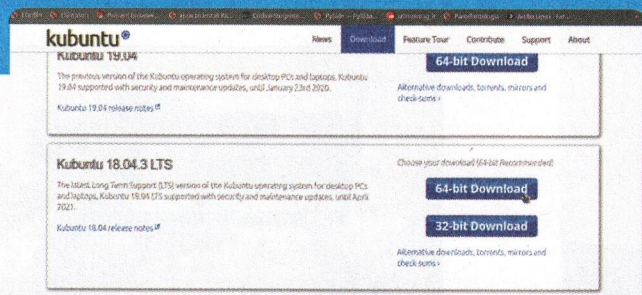
Sembra che la demo sia finita ma non è così perché nel "nuovo" menù generale ci sarà una nuova voce tremolante **Modalità Pro** sulla quale dovremo cliccare. Partirà di nuovo un video introduttivo al termine del quale cammineremo in avanti (tasto **W**) per iniziare la nostra avventura! Ricordiamo di utilizzare il tasto **M** per evidenziare la mappa di gioco!

WINDOWS 7 È MORTO: PASSA A LINUX

Microsoft ha ormai smesso di rilasciare aggiornamenti per Windows 7, uno dei sistemi operativi più apprezzati degli ultimi anni. E molti utenti non sono affatto contenti di passare a Windows 10. La soluzione perfetta? Passare a Kubuntu Linux

Dal 14 gennaio 2020 Windows 7, uno dei sistemi operativi Microsoft più apprezzati dagli utenti, non riceverà più aggiornamenti. Questo lo rende di fatto inutilizzabile, perché con il gran numero di malware in circolazione un sistema operativo non aggiornato finisce con l'essere troppo pericoloso. Basti pensare a quello che è successo ai vari utenti che avevano deciso di non lasciare Windows XP: i loro computer sono stati bloccati dai vari ransomware come Petya. E la storia dell'informatica ci insegna che lo stesso accadrà a Windows 7. In assenza di aggiornamenti, un sistema connesso a internet rischia la distruzione, e gli utenti rischiano di perdere tutti i propri dati personali o addirittura essere derubati. L'unica soluzione offerta da Microsoft è l'aggiornamento a Windows 10. Questo è, tuttavia, un sistema operativo non troppo popolare: le statistiche di StatCounter (***http://bit.ly/statistichewindowslinux***) ci ricordano che fino al dicembre 2019 Windows 7 ha ancora una diffusione del 26% su tutti i sistemi Windows, che è una bella fetta. Windows 10 ha la maggioranza, col 65%, ma è ancora troppo poco considerati gli sforzi di Microsoft per affievolire l'opposizione degli utenti. Le critiche sono tante (***http://bit.ly/win10critic***), dagli aggiornamenti esagerati alle difficoltà per non fornire un proprio indirizzo email e più in generale i dubbi riguardo il rispetto della privacy. Visto che però adesso tutti sono obbligati, per forza di cose, a cambiare sistema operativo, può essere una buona occasione per fare il passaggio definitivo a GNU/Linux. Chi si trova bene con l'interfaccia di Windows 7, e mal sopporta la prepotenza di Windows 10, può sentirsi a proprio agio con Kubuntu Linux. Con un sistema GNU/Linux il computer è infatti totalmente nelle mani dell'utente, e i dati personali sono al riparo

Scaricare il necessario

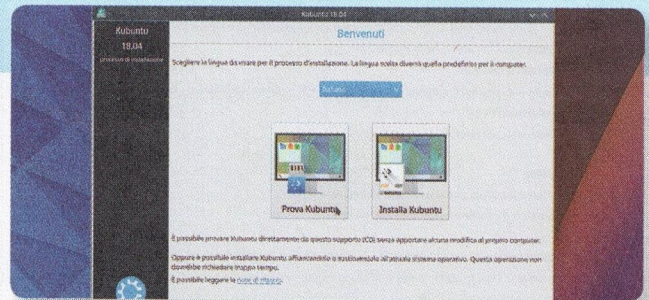
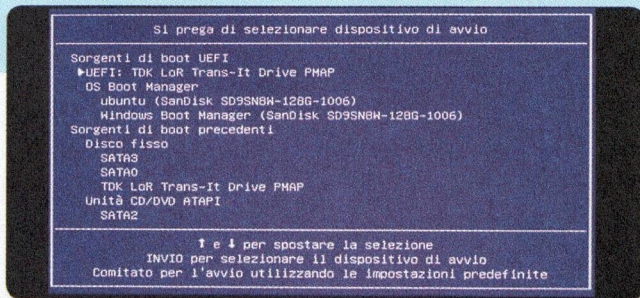
Otteniamo gratuitamente sia Kubuntu che il programma per caricarlo su una pendrive

01 IL DOWNLOAD

La prima cosa da fare è procurarsi Kubuntu: essendo un sistema libero e gratuito, basta andare sul sito web ***http://bit.ly/scaricakubuntu*** e scaricare la versione LTS (Long Term Support). Al momento è la versione 18.04.3, e conviene sceglierla perché è la più stabile.

02 SULLA PENDRIVE

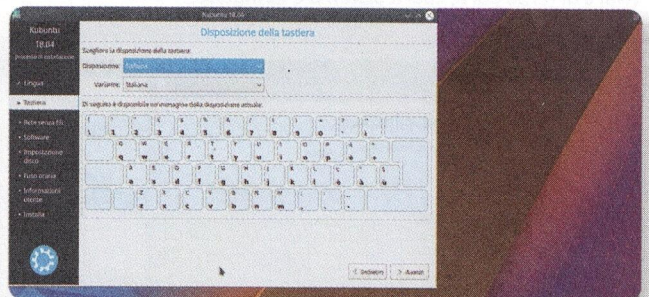
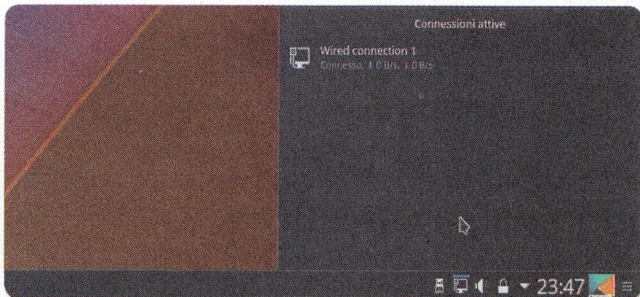
Serve poi un programma in grado di scrivere quell'immagine su una pendrive: Unetbootin è la soluzione perfetta per Windows. Basta scaricarlo da ***http://bit.ly/softwareunetbootin***, selezionare il file ISO di Kubuntu, e indicare l'unità USB.

Avviare il computer dalla pendrive

Usando il menù di avvio possiamo caricare il sistema Kubuntu installato nella chiave USB

01 AVVIO DA USB

Inserita la pendrive avviabile nel proprio PC, lo si può accendere premendo il tasto per il menù di avvio: di solito F9, F10, F2, o ESC. Alla comparsa del menù si sceglie la voce che indica la chiavetta USB, meglio se affiancata alla sigla UEFI.

02 QUALE LINGUA

Dopo qualche minuto, Kubuntu si sarà avviato. Ci viene subito chiesto di indicare la lingua che vogliamo utilizzare (l'Italiano, probabilmente), e scegliere se provare il sistema o installarlo subito: è meglio provarlo.

03 CONNESSIONE

Quando il desktop viene caricato si può facilmente configurare la rete con la tipica icona nella barra in basso a destra. Le schede ethernet sono riconosciute automaticamente, per il WiFi basta scegliere la rete e indicare la password

04 INSTALLAZIONE

Ora si può cliccare sull'icona presente sul desktop, chiamata **Install Kubuntu**. Tra le prime informazioni richiesta vi è la conferma della lingua da installare e della tastiera utilizzata: si potranno comunque aggiungere altre tastiere in seguito.

dai malintenzionati. Abbiamo quindi preparato un tutorial per installare l'ultima versione di Kubuntu su una pendrive, una chiavetta USB, da utilizzare in versione "live", senza modificare il PC. Inoltre, spieghiamo anche come installare il sistema su un hard disk e come personalizzare l'aspetto per farlo assomigliare il più possibile a Windows 7. Così anche chi non è a proprio agio con il dover imparare una nuova interfaccia potrà avere una transizione molto morbida verso GNU/Linux e la sua libertà e privacy.

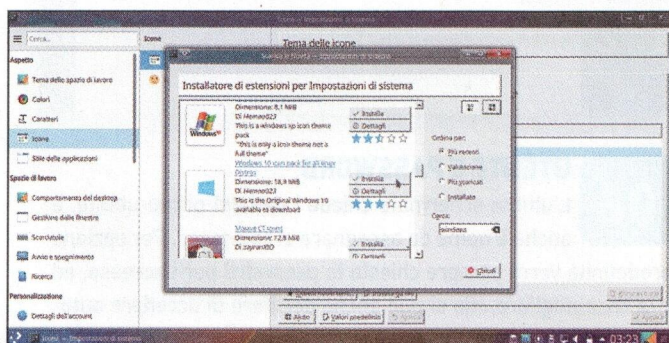
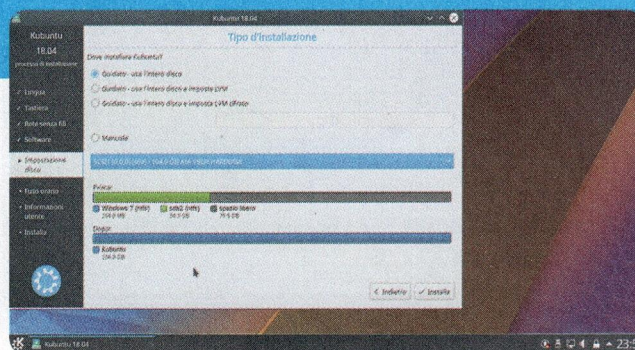
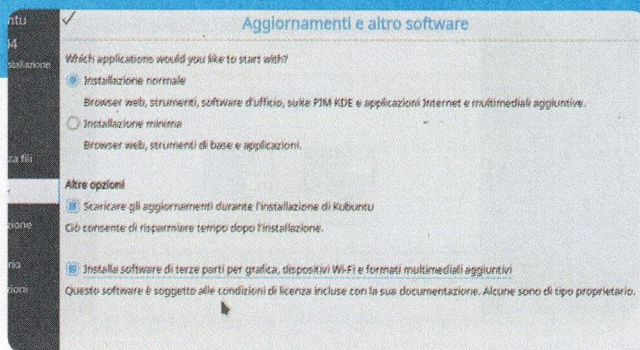



Fig. 1 • Per avere le icone in stile Windows si può andare in Impostazioni di sistema/Icone/Tema delle Icone e scegliere il "Windows 10 icon pack" dalla finestra Ottieni nuovi temi

IL CLONE DI WINDOWS 7

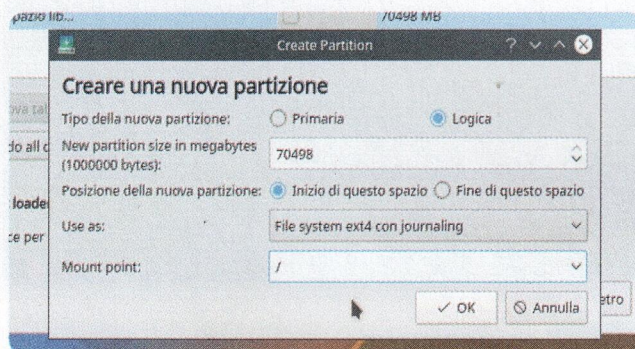
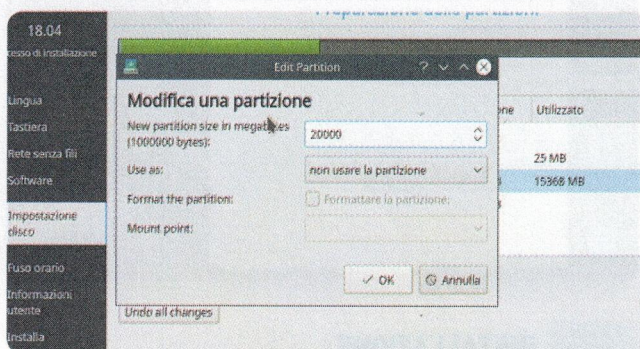
Per semplificare la vita ai meno esperti, abbiamo realizzato una nostra versione di Kubuntu, dotata dei principali programmi di uso comune e di una serie di temi grafici per farlo assomigliare il più possibile a Windows 7.
Si tratta di una versione di Kubuntu per gli utenti italiani: l'OS perfetto per una transizione indolore da Windows 7 a Kubuntu, provando comunque tutta la potenza dell'interfaccia grafica KDE. Questa versione, che abbiamo chiamato Anita, si trova nel DVD allegato. Provare per credere!!!

Installare Kubuntu sul PC

Possiamo installare Kubuntu in dual boot con Windows

01 INSTALLA TUTTO

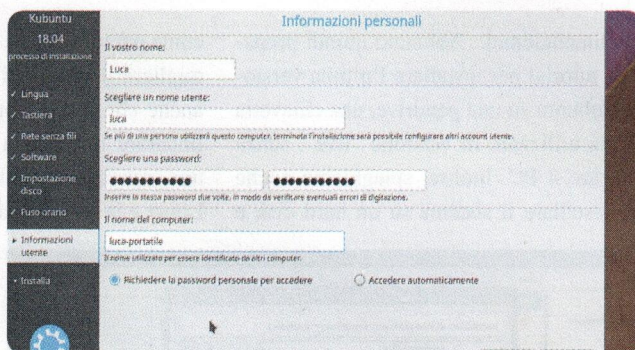
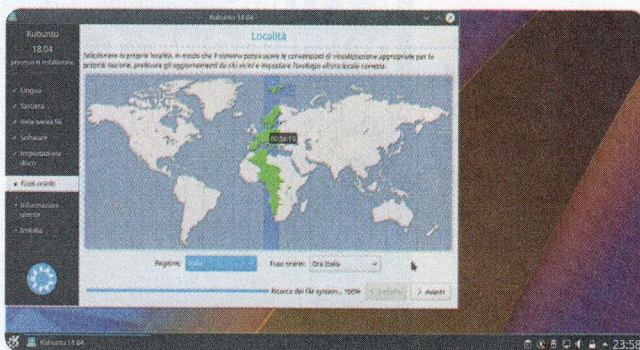
È poi importante scegliere che tipo di installazione fare: conviene una **Installazione normale**, mettendo la spunta alle opzioni per scaricare gli aggiornamenti e aggiungere software di terze parti, così il sistema è completo.

02 PARTIZIONAMENTO

Arriva ora il momento di partizionare il disco, l'unico momento delicato. Se non ci interessa più Windows e vogliamo cancellarlo, possiamo scegliere l'opzione **Guidato - usa l'intero disco**. Così il sistema farà tutto da solo.

03 RIDURRE WINDOWS

Se invece si vuole conservare Windows in dual boot bisogna procedere in modalità **Manuale**. Prima di tutto si clicca sulla partizione di Windows **(ntfs)** per ridurne la dimensione, in modo da creare lo spazio necessario a Kubuntu (qualche decina di GB).

04 NUOVA PARTIZIONE

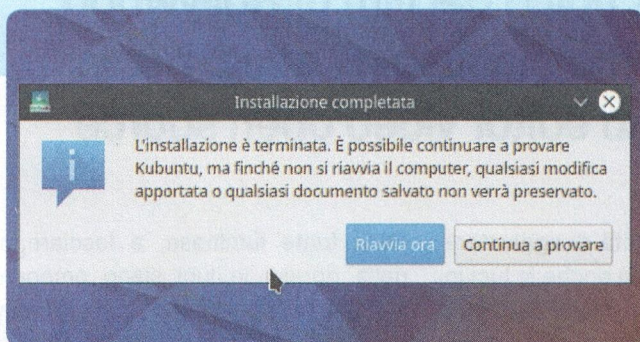
Nello spazio liberato è possibile creare una nuova partizione, che sarà automaticamente di tipo **ext4**. Nella casella **Mount point** si deve soltanto scrivere uno slash, il simbolo /. Alla fine, si preme il pulsante **Installa** per procedere.

05 IL FUSO ORARIO

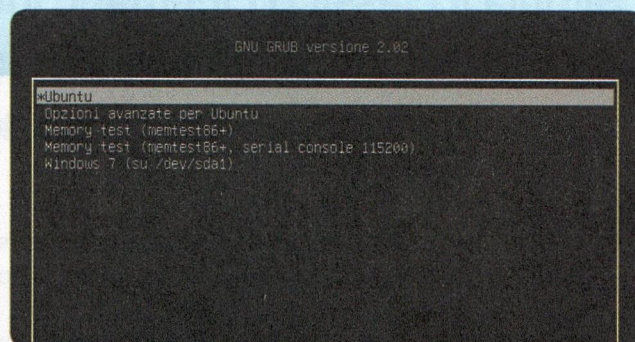
Il sistema viene già installato, ma vengono richieste ancora un paio di informazioni, per personalizzare l'installazione. La prima è il fuso orario: il sistema cercherà di capirlo automaticamente, ma possiamo anche indicare manualmente la zona giusta.

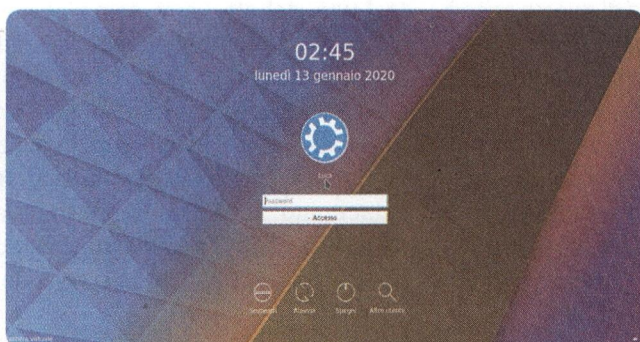
06 UTENTE E PASSWORD

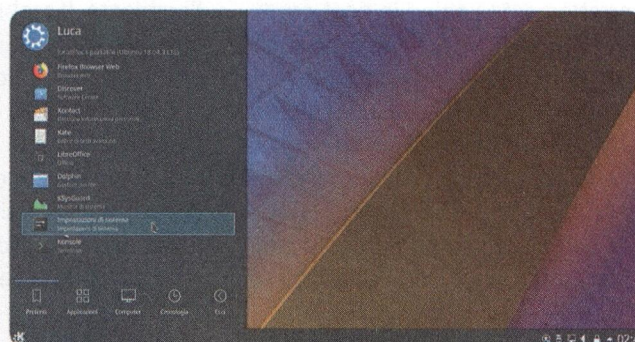
L'ultima schermata chiede i dati del primo utente, e anche il nome da assegnare al computer. Per opzione predefinita verrà sempre chiesta la password per l'accesso, ed è la cosa migliore, ma si può anche decidere di accedere automaticamente.

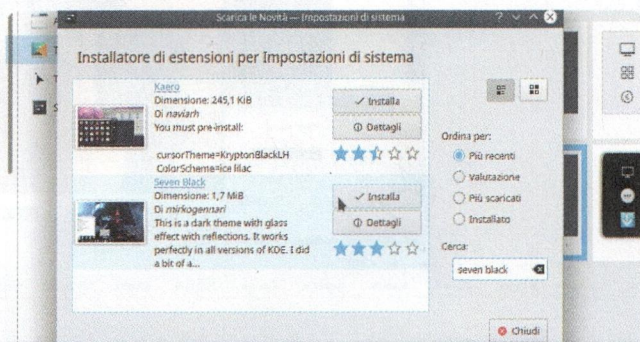
Il primo accesso

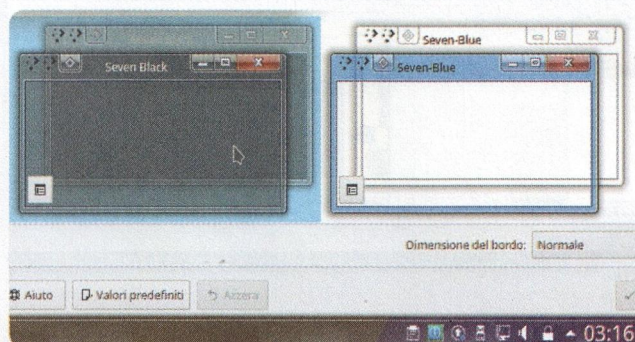
Accediamo per la prima volta a Kubuntu e personalizziamolo

01 PRIMO RIAVVIO

Alla fine dell'installazione il sistema propone il riavvio: se non abbiamo altre cose da fare conviene riavviare subito, per provare il nuovo sistema. Chiaramente, al riavvio potremo togliere la pendrive, ormai Kubuntu è sul PC.

02 IL BOOT LOADER

All'avvio vedremo una schermata nuova: si tratta del boot loader, che mostra la presenza dei vari sistemi operativi. Se abbiamo installato Kubuntu senza cancellare Windows li vedremo entrambe, e possiamo usare le frecce della tastiera per scegliere cosa avviare.

03 IL PRIMO LOGIN

Il primo avvio di Kubuntu può richiedere qualche minuto. Superata la schermata di login, sarà probabilmente necessario aspettare un altro po', due minuti al massimo, finché la configurazione del nostro utente viene completata.

04 DESKTOP PRONTO

Abbiamo finalmente il nostro Kubuntu: possiamo muoverci tra i vari pulsanti e le applicazioni del menù di avvio, rappresentato dal logo in basso a sinistra, come avviene anche nei vari sistemi Windows.

05 TEMA DEL DESKTOP

Per chi vuole un aspetto più simile a Windows, si può andare nelle **Impostazioni di sistema**, sezione **Tema dello spazio di lavoro/Tema del desktop**. Cliccando su **Ottieni nuovi temi**, si trova il tema **Seven Black**: basta scaricarlo e selezionarlo come predefinito.

06 LE DECORAZIONI

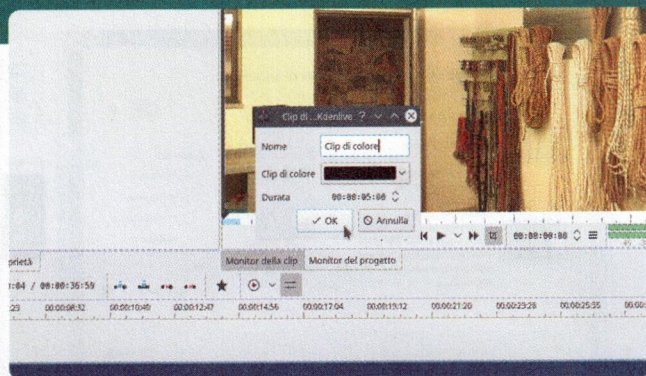
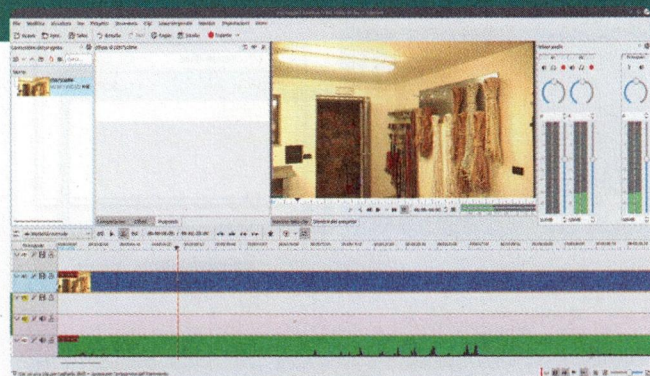
Sempre nelle **Impostazioni di sistema**, andiamo nella sezione **Stile delle applicazioni/Decorazioni delle finestre**, cliccando poi su **Scarica nuove decorazioni**. Qui è possibile trovare sia **Seven Black** che **Seven Blue**, abilitando quello che risulta più gradevole.

Un look cinematico

Simula il classico cinematic look tipico dei film di Hollywood: basta una ripresa leggermente sovraesposta e gli effetti per la manipolazione della luce del famoso editor video open source

Chi realizza cortometraggi solitamente cerca di raggiungere la qualità del grande cinema. Oggi le DSLR permettono di ottenere immagini molto buone in termini di gamma dinamica. La resa dei colori e della luminosità è però complicata: spesso i colori ottenuti dalle cineprese sembrano piatti, ma è solo perché l'immagine dovrebbe essere curata. Esiste infatti il color grading, che permette di bilanciare correttamente i colori in post produzione. Tuttavia, bisogna ricordare che il primo passo dovrebbe essere proprio l'illuminazione: usare una corretta illuminazione mentre si filma una scena permette di ottenere direttamente in camera il risultato desiderato. Naturalmente con mezzi amatoriali non è sempre facile ottenere il "look cinematico". Esiste però la possibilità di aggiustare non soltanto i colori ma anche le luci in post produzione. E lo si può fare con Kdenlive, sfruttando le sue modalità di sovrapposizione. Il problema tipico è la direzione della luce: quando si filma una scena in una stanza spesso non si hanno molte luci, soprattutto luci facilmente regolabili, quindi si finisce con l'utilizzare un semplice lampadario che illumina in modo uniforme un po' tutto l'ambiente. Il problema di questa cosa è che distrae molto lo spettatore: è bene che si veda un po' tutta la scena, ma l'attenzione deve essere diretta verso l'attore e ciò che sta facendo. Insomma, servirebbe una sorta di riflettore, anche se non così marcato come quelli dei teatri. La soluzione consiste nel riprendere l'attore non troppo lontano dalla fonte luminosa, e lasciare che nella ripresa le luci siano omogenee in tutta la stanza. Poi, con Kdenlive, possiamo creare una cortina nera con cui coprire tutte le parti dell'immagine in cui non vogliamo che ci sia molta luce. Ovviamente la sorgente luminosa e l'attore devono essere ben illuminati, ma per il resto possiamo "nascondere" quello che vogliamo. Sovrapponendo questo blocco nero con la modalità **Luce debole** verrà semplicemente abbassata la luminosità dell'area interessata. Questo ci permette di fatto di rimodellare la luce, perché possiamo scegliere l'area da mettere in ombra con molta cura grazie all'effetto **Rotscoping**. Il trucco, infatti, consiste nel creare un rettangolo nero che copre tutta la clip, e poi ritagliare via solo la

Due clip sono sufficienti

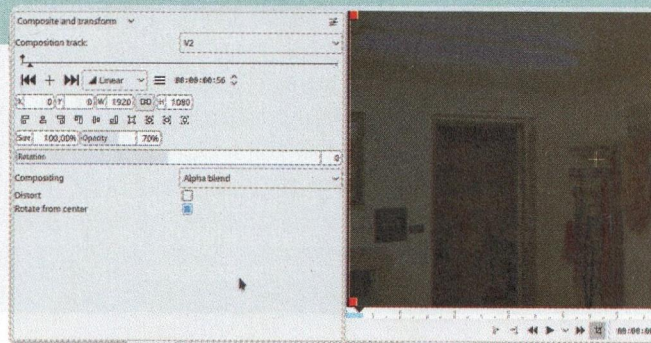
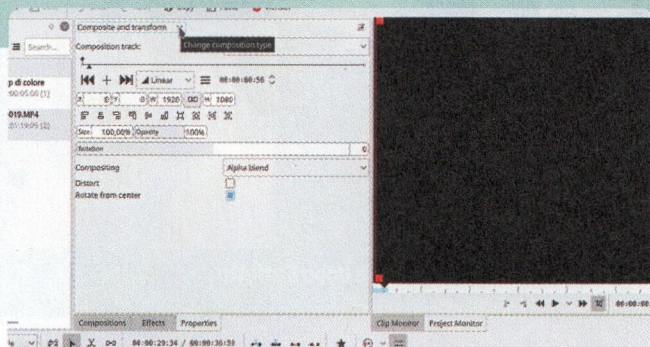
Per l'effetto ci servono solo il filmato e una clip completamente nera

01 UNA CLIP VIDEO

La prima cosa da fare è partire dalla clip video che abbiamo filmato: bisogna caricarla in Kdenlive e eventualmente tagliarla se necessario. La clip può essere caricata nella traccia video più bassa, di solito la **Video1**.

02 CLIP TINTA UNITA

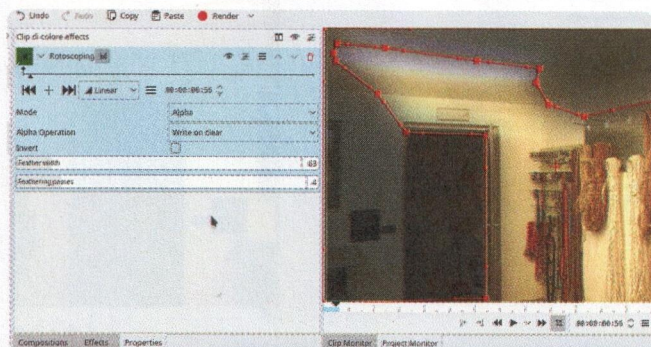
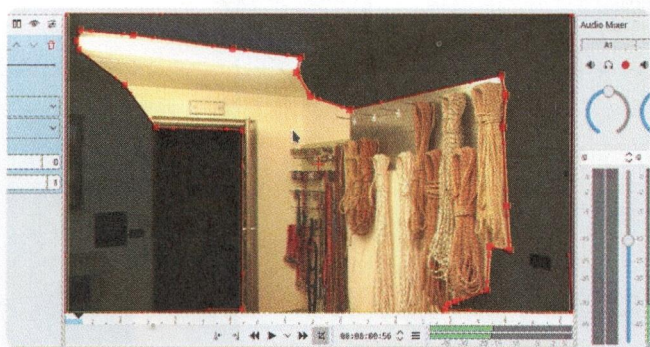
Nella traccia video immediatamente superiore, quindi la **Video2**, possiamo caricare una clip colore completamente nera. Per crearne una basta andare nel menù **Project/ Color clip**, selezionando il colore nero.

Il percorso della luce

Disegniamo il contorno dell'area che deve essere illuminata

01 LA TRANSIZIONE

La clip di colore nero va allungata, finché si sovrappone (come durata) perfettamente al video. Tra le due clip si deve aggiungere una transizione di tipo **Composite and transform**. La transizione deve ricoprire tutta la durata di entrambe le clip.

02 L'ALPHA BLEND

Questa transizione può avere, per ora, il metodo di composizione **Alpha blend**. L'opacità deve essere ridotta al **70%**, in modo da poter vedere il filmato originale. Dipende ovviamente da quanto luminosa è la propria immagine di partenza.

03 COL ROTOSCOPING

Ora aggiungiamo l'effetto **rotoscoping** di colore nero. Cliccando col tasto sinistro sull'immagine dobbiamo disegnare il percorso della luce, ma al contrario: dovrà essere selezionato tutto ciò che non è colpito direttamente dalla luce.

04 BORDO SFUMATO

È poco intuitivo, ma l'obiettivo è oscurare le parti del filmato che non sono al centro dell'attenzione. Finito ciò si può chiudere il disegno col tasto destro del mouse. Impostiamo **feather** da 60 punti e **4 feather passes**, per una sfumatura morbida.

parte che deve essere ben illuminata. Sfruttando la sfumatura del rotoscope è possibile avere un ottimo gradiente. Chiaramente, per la riuscita dell'effetto è importante seguire una certa logica: bisogna seguire il contorno degli oggetti, per dare un senso della tridimensionalità. Per esempio, se c'è un tavolo in primo piano questo dovrà essere completamente dentro o fuori dal ritaglio, ma non potrà stare a metà strada. Con un paio di altre correzioni è poi possibile aggiustare tutti i piccoli dettagli sovraesposti o sottoesposti. L'esempio lo trovi su ***http://bit.ly/esempiocinema***

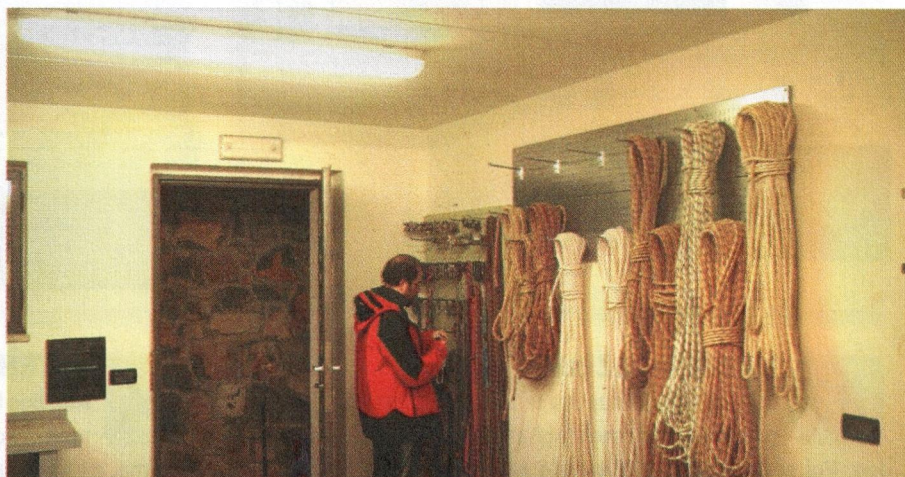



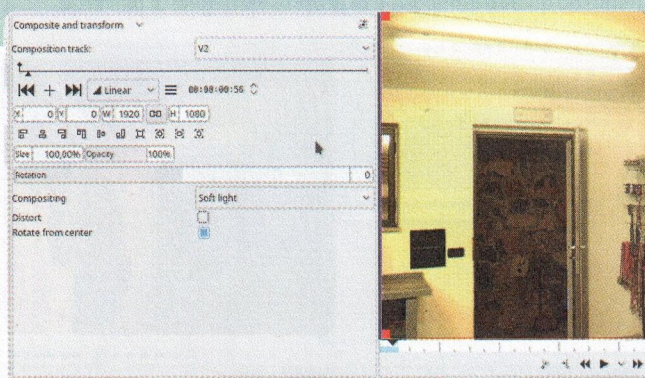
Fig. 1 • L'immagine da cui siamo partiti

UNA SCENA SOVRAESPOSTA

Per lavorare sui colori e la luminosità di una scena è importante cercare di riprenderla con una cinepresa capace di registrare una notevole gamma. In secondo luogo, è anche bene poter regolare manualmente l'esposizione. Questo perché per l'effetto che vogliamo ottenere è bene avere una immagine leggermente sovraesposta. La sovraesposizione deve essere lieve, altrimenti le alte luci risulteranno bruciate. Avere molta luce è però importante per evitare che l'aumento delle ombre che realizziamo in post produzione renda del tutto nera buona parte della scena. Per il resto, è importante cercare di tenere gli attori sempre nella stessa parte della scena, così da evitare che entrino nell'area che verrà resa più scura.

■ **Fig. 2 • La stessa immagine dopo l'effetto**

Correggere il colore

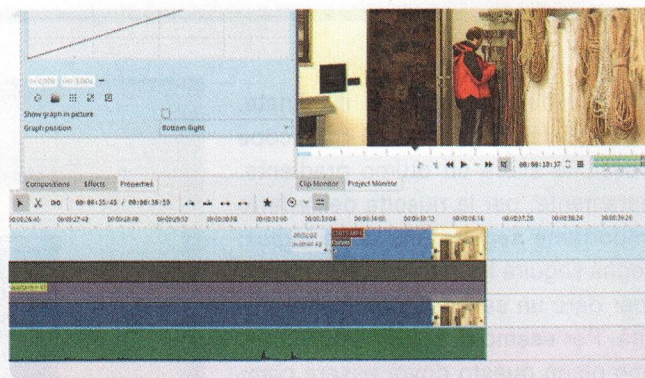
Aggiustiamo i colori tra ombre e mezzitoni

01 MASSIMA OPACITÀ

Tornando a lavorare sulla transizione, impostiamo la modalità di sovrapposizione a **Soft light**. L'opacità deve poi essere alzata: idealmente dovrebbe andare al 100%, ma la si può tenere un po' più bassa se l'alone d'ombra è troppo marcato.

02 MENO SATURAZIONE

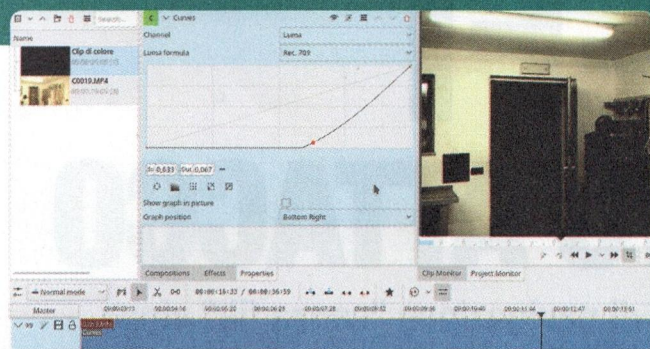
Aggiungiamo alla clip del filmato originale un effetto **Curves**, sul canale **Saturation**. L'idea è di mantenere la saturazione normale (sulla diagonale) per alte luci e mezzitoni, abbassandola per le ombre, che quindi risulteranno meno colorate.

03 LA DUPLICAZIONE

Ora possiamo duplicare la clip originale: il primo passo consiste nel tagliare un pezzo della clip video. Poi si deve spostare questo pezzo nella traccia libera sopra le altre, la **Video3**, mantenendo l'allineamento.

04 ESTENDERE LE CLIP

Alla fine basta estendere le due clip: quella originale, nella traccia **Video1**, tornerà a avere la stessa durata di prima, e l'altra (traccia **Video3**) dovrà essere allungata nella direzione opposta in modo da essere identica a quella originale.

La luce giusta ai dettagli

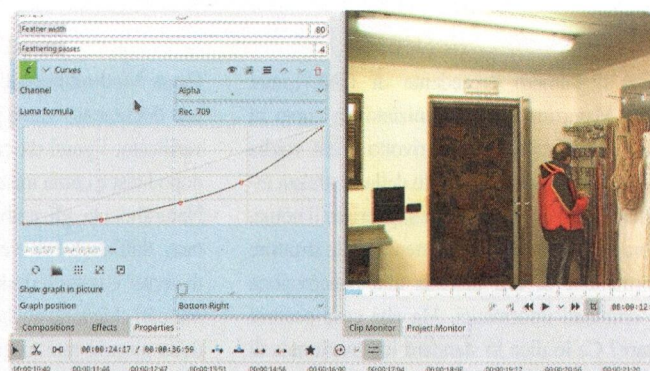
Con il rotoscope possiamo fare ritocchi ai dettagli "fuori posto"

01 CURVE DI LUCE

La nuova clip **Video3**, essendo un clone della clip presente in **Video1,** ha tutti i suoi effetti: rimuoviamoli e inseriamo solo un effetto di tipo **Curves** sul canale **Luma**. Dobbiamo abbassare la luminosità per vedere bene gli oggetti sovraesposti.

02 UNA TRANSIZIONE

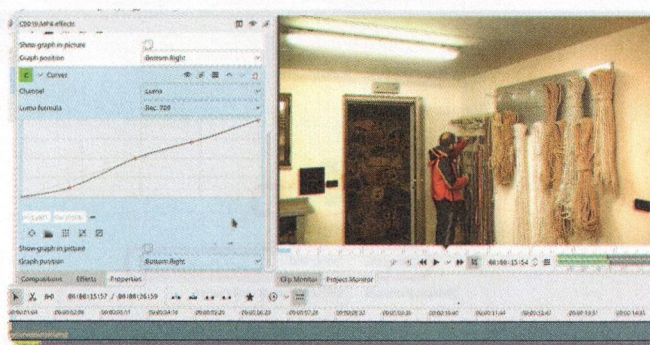
Aggiungiamo una transizione per tutta la durata di questa clip: la transizione deve essere di tipo **Composite and transform**, e riferita alla traccia **Video1**. Per il resto, va bene la modalità **Alpha blend** con opacità al **100%**.

03 IL ROTOSCOPING

Aggiungiamo sempre a questa clip un effetto di tipo **Rotoscoping,** selezionando il contorno dell'oggetto che nella ripresa originale risulta sovraesposto, per esempio il soffitto. Utilizziamo un **feather** di almeno **80**, così da sfumare bene i bordi.

04 CANALE ALPHA

Probabilmente abbiamo ancora ombre troppo forti. Per ottenere una migliore fusione, aggiungiamo l'effetto **Curves** sul canale Alpha, abbassando molto le ombre, e gradualmente il resto (senza però diminuire troppo le alte luci).

05 ALTRI OGGETTI

Naturalmente, è probabile che siano presenti altri oggetti sovraesposti: possiamo aggiungere anche questi creando un nuovo effetto **Rotoscoping** con **Alpha operation** impostata a **Maximum** e ritagliando il contorno di un oggetto sovraesposto.

06 MENO CONTRASTO

Alla fine è possibile aggiustare l'immagine originale nel complesso, inserendo un effetto **Curves** nella clip della traccia **Video1**. L'effetto deve lavorare sul canale **Luma** e alzare leggermente i mezzitoni, abbassando un po' le ombre.

PEN TESTING - *Parte 2*

WI-FI SOTTO ATTACCO

Se la modalità di navigazione "senza fili" vince un'ipotetica gara di "comodità", non si può dire la stessa cosa sulla sicurezza, soprattutto in presenza di errate implementazioni

Michele Petrecca

Sul numero precedente di GNU/Linux Magazine abbiamo iniziato un corso di Penetration Testing, rivolto a chi voglia provare a lavorare nell'ambito della sicurezza informatica. Il PenTester, come suggerisce il nome, lavora infatti testando la resistenza delle strutture informatiche di una azienda alla penetrazione dei criminali informatici. Ma che cosa occorre testare? Ce lo dice lo standard internazionale di riferimento per l'esecuzione delle verifiche di sicurezza nel documento – in allegato nel DVD – **The Open Source Security Testing Methodology Manual** versione 3 dell'associazione no-profit **ISECOM** (**Institute for Security and Open Methodologies** – ***http://bit.ly/isecom***). In tale documento viene indicato cosa deve essere verificato, i passi da compiere prima, durante e dopo i test e come misurare i risultati ottenuti. Naturalmente gli ambiti in cui muoversi sono tanti, dall'analisi di web abb al controllo remoto di server e sistemi desktop. Ma non solo: i committenti chiedono anche di verificare la sicurezza della propria rete aziendale. Tutti gli uffici, infatti, sono ormai dotati di WiFi, perché è molto economico e permette ai dipendenti di utilizzare anche tablet o altri dispositivi per il proprio lavoro. Tuttavia, un eventuale malintenzionato potrebbe sfruttare il raggio del WiFi per avvicinarsi fisicamente alla sede dell'azienda e entrare nella rete, cercando di carpire informazioni sensibili. È per questo motivo che bisogna avere una certa pratica di come funzionino le reti WiFi.

Fig. 1 • Valori preconfigurati in un tipico router domestico

DUE FALLE CLAMOROSE

Non possiamo non ricordare due problemi che diedero non poco filo da torcere a tutti i sistemi operativi (GNU/Linux compreso!) basando la propria "fortuna" sulle tecnologie wireless, nello specifico Bluetooth e Wi-Fi. Lo stack Bluetooth andò sotto attacco della tecnica **Blueborne** scoperta dai laboratori **Armis** (***http://bit.ly/armisblueborne***): una falla dovuta ad un **buffer overflow** al livello di implementazione software del protocollo permetteva ad un malintenzionato di catturare informazioni fino alla possibilità di eseguire codice malevolo da remoto per tutti i device bluetooth che si trovassero nel proprio raggio d'azione e senza che la vittima si accorgesse che il proprio dispositivo fosse stato violato. La cosa "di per se" non sarebbe preoccupante se non fosse per il fatto che si sta parlando di svariati miliardi di dispositivi bluetooth sparsi in tutto il mondo e in quanto tale anche l'**IoT** (**Internet of Things**) non ne è stata immune! I curiosi possono approfondire andando sul sito del **Common Vulnerabilities and Exposures** (**CVE** - ***http://bit.ly/cvemitre***) quindi cliccare su **Search CVE List** e inserire prima **CVE-2017-1000250** per poi fare la ricerca con **CVE-2017-1000250**. È disponibile anche un **PoC** (**Proof of Concept**,

tecnica dimostrabile solo in determinate condizioni) rilasciato da **Armis** su **Github** all'indirizzo ***http://bit.ly/armisblueborne source***.

Da allora sono state rilasciate le patch necessarie, ad esempio **BlueZ** (***http://bit.ly/bluezorg***) che implementa lo stack in GNU/Linux rilasciò subito la versione 5.47, ma questo non vuol dire che non siano presenti altre vulnerabilità come oltremodo dimostrano i successivi rilasci di BlueZ, in versione 5.52 al momento di scrivere. Per certi versi ancora più clamoroso – poiché era ritenuto estremamente sicuro – è l'attacco al protocollo **WPA2** (**Wi-Fi Protected Access II**), attacco meglio noto con il nome **KRACK** (contrazione/acronimo di **Key Reinstallation AttaCK**) scoperto dai Belgi **Mathy Vanhoef** e **Frank Piessens** e dettagliatamente descritto nel loro paper **Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2** presente nel DVD allegato e a cui si rimanda per i dovuti approfondimenti.

COME FUNZIONA

Proviamo a spiegare in maniera semplificata la dinamica del **4 Way Handshake**, il protocollo Wi-Fi vulnerabile all'attacco KRACK. Immaginiamo lo scenario che vede i dati Internet arrivare al nostro router di casa. Fino a che non ci colleghiamo al router non potremo effettuare alcuna connessione a Internet. Escludiamo in questo contesto l'utilizzo del cavo ethernet, nel qual caso il problema non sussisterebbe, e ipotizziamo di collegarci con il portatile e/o lo smartphone via Wi-Fi. Nel preciso istante in cui iniziamo il collegamento parte un scambio di dati tra il dispositivo client che richiede la connessione (detto **Supplicant**) e chi la deve concedere l'**AP** (**Access Point** detto anche **authenticator**) presente nel router. Lo scambio dati avviene secondo precise sequenze dettate dal protocollo WPA2. Prima di tutto ricordiamo che i **Supplicant** vengono a conoscenza della presenza di un **AP** poiché quest'ultimo periodicamente invia un **beacon frame**, in sostanza un messaggio sulle caratteristiche della rete nell'area che riesce a coprire al fine di annunciarne la presenza. In alcuni AP è possibile impostare tale tempo intervenendo sulla variabile **Target Beacon Transmission Time** (**TBTT**): in genere di default è impostata a **100TU** ed essendo **1TU=1024µs** è evidente come l'intervallo di trasmissione tra un frame e un altro sia poco più di **100ms**. In questa fase preliminare di richiesta di autenticazione e associazione viene generata la chiave di sessione **PMK** (**Pairwise Master Key**) uguale per tutti i client poiché ottenuta da una coppia di elementi preconfigurati (Figura 1): la **PSK** (**Pre Shared Key** (in genere la passphrase) e il **SSID** (**Service Set IDentifier**) vengono dati in pasto come argomenti alla funzione di derivazione crittografica **PBKDF2** (**Password-Based Key Derivation Function 2**) la quale, dopo essere stata applicata per 4096 volte, fornisce la **PMK** da 256bit il tutto in maniera trasparente all'utente. In ambiente corporate/industriale la procedura è differente: per semplificare, troviamo un **AP** associato ad un server **RADIUS** con annesso database e la **PSK** è diversa per ogni **Supplicant**, viene generata di volta in volta all'atto della connessione ed è valida solo per quella sessione.

Dopo la fase preliminare inizia la dinamica del protocollo **4 Way Handshake** (Figura 2). Nel primo messaggio l'**AP** invia al **Supplicant** un **ANonce**, numero pseudo-casuale da 256bit. Alla ricezione il **Supplicant** genererà un proprio numero pseudo-casuale da 256bit (**SNonce**) e la chiave **PTK** (**Pairwise Transit Key**) che verrà utilizzata in seguito per cifrare/decifrare il traffico. La suddetta chiave viene generata applicando la funzione:

```
PTK=PRF[PMK+ANonce+ SNonce+
        MAC(AP)+MAC(Supplicant)]
```

laddove **PRF** è una funzione pseudo-casuale (**Pseudo Random Function**) che prende come argomenti anche i MAC address del Supplicant e dell'AP. Generata la PTK il Supplicant effettua il secondo passaggio previsto dal protocollo generando un messaggio da inviare all'**AP** contenente il **SNonce** e il **MIC** (**Message Integrity Code**), un valore – calcolato utilizzando la **KCK** (**Key Confirmation Key**) contenuta nel primo campo della **PTK** – che garantisce l'integrità e l'autenticazione di un messaggio digitale. Ad essere pignoli il **MIC** dovrebbe indicarsi con **MAC** (**Message Authentication Code**), da non confondere con l'indirizzo **MAC** (**Media Access Control**) univoco di un dispositivo. Possiamo notare come, per aumentare la sicurezza, la chiave PTK non venga mai trasmessa nell'etere, ma l'AP la ricava alla ricezione del messaggio dal Supplicant.

A questo punto l'AP e il Supplicant hanno la stessa chiave PTK: l'AP genererà la chiave **GTK** (Leggere il box "**Chiave di gruppo**") a cui farà seguito il terzo passaggio del protocollo che consiste fondamentalmente in un modo per comunicare informazioni di sicurezza tra le stazioni, di fatto una validazione/verifica implementata con **RSN IE** (**Robust Security Network - Information Element**) a cui viene aggiunta la chiave GTK il tutto protetto con il valore **MIC**. Il Supplicant ricevendo il messaggio installerà le chiavi PTK e GTK quindi invierà un ACK che confermerà all'AP che entrambi – AP e Supplicant – hanno le stesse chiavi PTK e GTK. A questo punto inizia la trasmissione cifrata tra AP e Supplicant in base allo schema – di principio e semplificato – riportato in Figura 3 e sulla base della quale occorre fare alcune osservazioni.

WPA2, rispetto ai suoi predecessori in particolar modo al vecchio **WEP** (**Wired Equivalen-**

LA PRATICA CON KALI

Mettere alla prova il proprio router

Sono stati pubblicati su GitHub (***http://bit.ly/krackattacks***) script e istruzioni per testare la propria rete. Non si tratta di script per eseguire un attacco vero e proprio, per poterli usare è comunque necessario conoscere la chiave WPA di accesso della rete WiFi da testare. Servono infatti solo per verificare se i propri dispositivi WiFi siano vulnerabili. Non presentiamo qui le varie istruzioni per l'uso degli script per due motivi. Il primo è che sono molto semplici, si tratta solo di eseguire un paio di comandi e aspettare che lo script faccia tutto da solo. Il secondo motivo è che per il momento sono anche abbastanza inutili: il metodo più semplice e veloce per capire se un dispositivo è vulnerabile è guardare la sua data di aggiornamento (del firmware o dei driver WiFi). Se il firmware è precedente al 2019 il dispositivo è certamente vulnerabile, visto che le prime correzioni sono arrivate verso la fine del 2018. Lo script per eseguire il vero e proprio attacco verrà pubblicato sul repository GitHub quando gli autori riterranno che tutti abbiano avuto il tempo di aggiornare i propri dispositivi, probabilmente verso la fine del 2020.

CHIAVE DI GRUPPO

Traffico multicast/broadcast

Generata solo ed esclusivamente dall'**AP** e trasmessa al Supplicant nel terzo passaggio del protocollo 4 Way Handshake, la **GTK (Group Temporal Key)** è usata per cifrare tutte le trasmissioni broadcast/ multicast tra l'AP e tutti i dispositivi client associati allo steso AP. Per ogni AP ci sarà una GTK diversa che verrà condivisa con i relativi dispositivi associati (client).
La GTK dipende da una chiave di livello superiore, la **GMK (Group Master Key)** da 256bit la cui generazione è basata sul MAC address dell'AP e su un numero pseudo-casuale (**GNonce**).

te Privacy), ha introdotto il robusto protocollo di crittografia **CCMP** (**Counter-Mode/CBC-Mac Protocol**) che utilizza chiavi di crittografia **AES** (**Advanced Encryption Standard**) a 128 bit. Questa operazione applicata alla combinazione **Nonce** e **PTK** genera un **KeyStream** (flusso di bit pseudo-casuali) che combinato – bit per bit – in **XOR** (simbolo ⊕) con il **PlainText** (dati in chiaro) genera il messaggio cifrato. Da un punto di vista analitico per il primo pacchetto cifrato avremo **DC1=PT1⊕KS1**, per il secondo pacchetto **DC2=PT2⊕KS2** ecc. Ora se **Nonce1=Nonce2** si sta utilizzando lo stesso packet number che porterà a **KS1=KS2** nel qual caso, ricordando la funzione XOR, risulterà che **DC1⊕DC2=PT1⊕PT2** azzerando così l'effetto della cifratura. In sostanza se **PT1** è noto sarà possibile decifrare **PT2**. Morale del discorso, chi trasmette non deve mai utilizzare lo stesso **packet number** (**Nonce**)! Infine, la sigla **EAPoL** nelle figure indica uno scambio di informazione con messaggi **EAPoL–Key Frames** (**Extensible Authentication Protocol over LAN**) un metodo per trasportare i pacchetti **EAP** (**Extensible Authentication Protocol** - ***http://bit.ly/rfc3748***) tra Supplicant e AP direttamente tramite il servizio MAC LAN (sia cablato che wireless). Nel WPA2 è prevista l'autenticazione **EAP/PSK** e si rimanda all'**RFC** (**Request for Comment**) ***http://bit.ly/rfc4764*** per gli approfondimenti del caso. A questo punto conosciamo, in maniera non superficiale, la dinamica dietro un collegamento Wi-Fi.

ATTACCO AL WPA2

Riassumendo, quando un client si connette alla rete WPA2 dopo l'autenticazione sono necessari 4 passaggi per ottenere un canale cifrato. La chiave di cifratura è scambiata al passaggio 3, ed è proprio il terzo passaggio la parte vulnerabile del 4-way handshake, dove il pirata potrebbe intervenire con una tecnica definita **nonce reuse** che non si riferisce ai valori **ANonce** o **SNonce** bensì fa riferimento al numero del pacchetto trasmesso: il primo pacchetto avrà Nonce 0, il secondo Nonce 1 ecc. Anticipiamo subito che l'attacco non può avvenire via Internet, ma può essere eseguito solo nel raggio d'azione della rete Wi-Fi a cui è collegata la "vittima". Trattasi di un attacco **MitM** (**Man in the Middle**, Figura 4) nel quale il primo passo del pirata sarà realizzare un attacco **channel-based** clonando l'AP su un diverso canale. Questo tipo di attacco non decifrerà alcun dato, ma sarà indispensabile al pirata per intercettare tutti i messaggi al fine di effettuarne l'inoltro o il blocco a seconda delle condizioni.
Il malintenzionato lascerà passare i primi 3 frame del protocollo incriminato e quando il Supplicant invierà il 4° frame lo bloccherà. A questo punto il client avendo inviato il 4° messaggio, e non essendo più necessaria una risposta dall'AP, crederà che il 4-Way Handshake abbia avuto successo e installerà le chiavi PTK e GTK. Dal punto di vista dell'AP questo non è

Fig. 2 • Messaggi scambiati tra AP e client

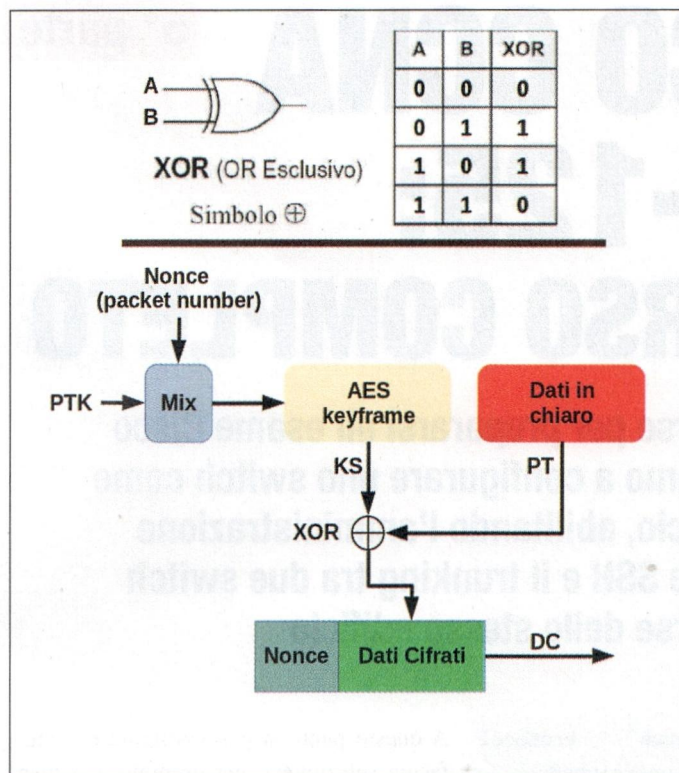



Fig. 3 • In alto la funzione XOR, in basso la cifratura dei pacchetti WAP2

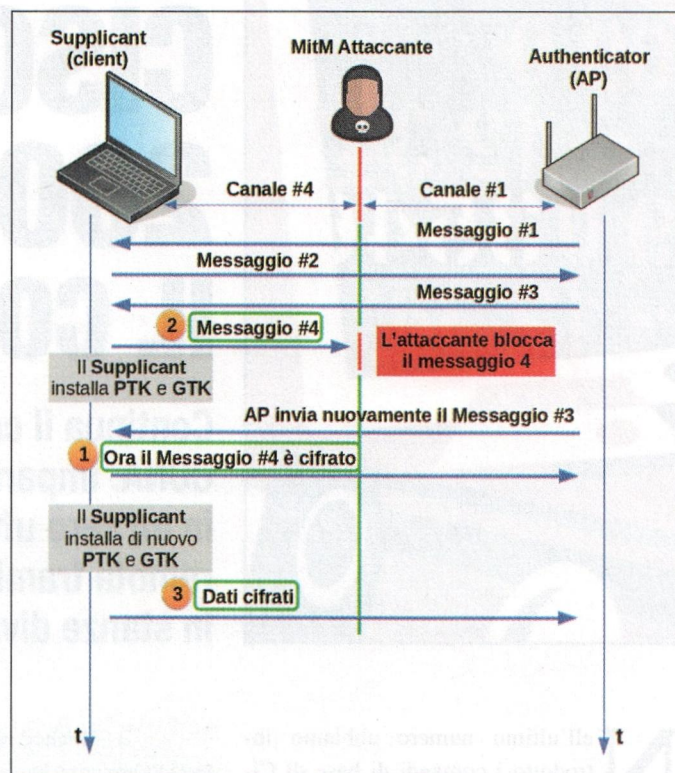
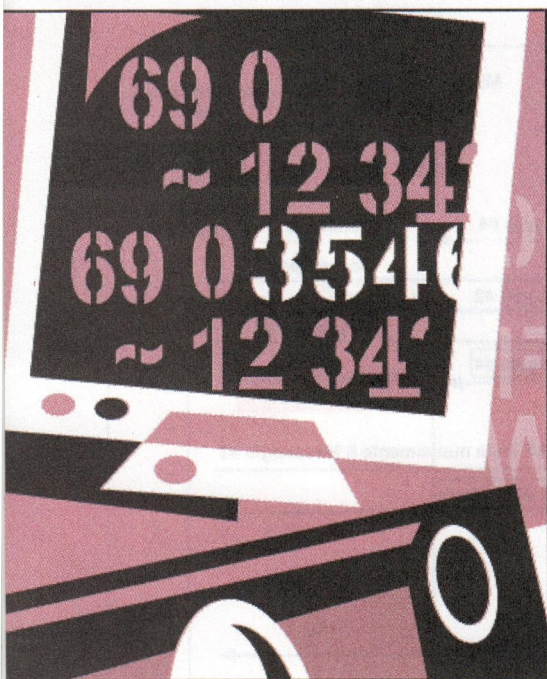



Fig. 4 • Dinamica dell'attacco KRACK al protocollo WPA2

vero perché essendo stato bloccato il 4° frame l'AP crede che il Supplicant non abbia ricevuto il 3° frame. Lo standard WPA2 prevede che il 3° frame possa essere ritrasmesso più volte – ad esempio per ovviare all'ipotesi in cui il client non riesca a riceverlo – e di ciò l'AP se ne rende conto quando non riceve il 4° frame di ACK. Come risultato l'AP invia nuovamente il 3° frame che verrà accettato dal Supplicant il quale replicherà all'AP con un altro 4° frame ma questa volta cifrato con la chiave PTK accettata in precedenza questo perché il Supplicant non sa che il suo precedente 4° frame gli è stato bloccato pertanto il secondo invio del 3° frame lo considera di fatto un dato con Nonce 1 e cifrandolo con la chiave precedentemente installata. Ma poiché il Supplicant sta rispondendo con un secondo 4° frame ecco che installerà nuovamente le chiavi PTK e GTK ed è proprio qui che avviene il danno poiché il **Nonce** (numero pacchetto) verrà di nuovo azzerato! A questo punto il primo data frame inviato dal Supplicant avrà Nonce pari a 1 esattamente lo stesso valore che aveva il secondo invio del 4° frame. Da qui il nome dell'attacco **nonce reuse**. Questa apparente banalità di riutilizzo del Nonce porta alla decriptazione dei dati esattamente come riportato nella descrizione della Figura 3.

Infatti, con riferimento ai numeri nei pallini coloro arancio di Figura 4 risulta che **1⊕2** da come risultato **KS** con **Nonce 1**. Ma con Nonce 1 vi sono anche i dati cifrati che il Supplicant invia dopo aver reinstallato le chiavi PTK e GTK. Allora effettuando **KS Nonce 1⊕3** si ottiene il danno, ovvero la decriptazione dei dati! E l'operazione di XOR (come visibile in Figura 2) è una operazione bit a bit che anche un microcontrollore su scheda Arduino riesce ad attuare e computare senza alcuna difficoltà! Va detto, a malincuore, che l'attacco è piuttosto insidioso su sistemi GNU/Linux, OpenBSD e Android poiché seguono alla lettera gli standard, mentre sembrano cavarsela egregiamente Windows e iOS, che non ci si adeguano strettamente. Ancor di più se consideriamo che l'implementazione tipica dei suddetti sistemi operativi si affida al software **wpa_supplicant** il quale installava una chiave di cifratura con tutti zero se attaccato, problema risolto – almeno questo – con il rilascio della versione **2.7** (***http://bit.ly/wifisec2017-1***).

CONCLUSIONI

Collegandoci al paragrafo introduttivo, quali azioni compiere per mitigare o, se possibile, eliminare il problema? Non esistono vere e proprie contromisure per questa vulnerabilità poiché il problema è insito nel protocollo stesso! Cambiare le password non serve a nulla, influenzerà solo la creazione della PSK, ma il problema non è nella PSK! Alcune misure che possono mitigare il problema vedono l'installazione di tutte le patch di sicurezza sui client e possibilmente l'uso di una **VPN** (**Virtual Private Network**). Se presenti disabilitare nel router sempre le voci **TKIP** (**Temporal Key Integrity Protocol**) e **GCMP** (**Galois Counter Mode Protocol**) e accertarsi di utilizzare sempre **AES-CCMP**. Spegnere il Wi-Fi dell'AP quando non in uso. Aggiornare i firmware degli AP e verificare se è possibile disabilitare la ritrasmissione del terzo messaggio, il vero cuore del problema! Ma non tutti gli apparati sono aggiornabili e tra quelli aggiornabili non tutti hanno (o danno) la possibilità di cambiare alcuni aspetti del protocollo. Se trattasi di router domestici poco male, il raggio d'azione difficilmente supera le mura di casa ma una verifica andrebbe sempre fatta per gli ambienti corporate/industraili e tra i dispositivi che offrono Wi-Fi libero. Diversi **Vendor** hanno fornito patch e contromisure, per un elenco è sufficiente puntare il browser all'indirizzo ***http://bit.ly/krackinfovrc***.

CISCO CCNA 200-125: IL CORSO COMPLETO

5° parte

Continua il corso per prepararsi all'esame Cisco CCNA: impariamo a configurare uno switch come in un vero ufficio, abilitando l'amministrazione remota tramite SSH e il trunking tra due switch in stanze diverse dello stesso edificio

Nell'ultimo numero abbiamo introdotto i comandi di base di Cisco IOS, il sistema operativo dei dispositivi di rete Cisco, e abbiamo preso confidenza con le varie modalità. I comandi di IOS infatti devono essere lanciati dalla giusta modalità, altrimenti non vengono riconosciuti. Bisogna ragionare in termini di contesto: in ogni contesto si possono fare alcune cose. Nel contesto della configurazione globale si possono impostare dati come l'hostname, nel contesto di una porta ethernet o virtuale si può configurare se sia abilitata o meno. Adesso, però, bisogna pensare ai vari comandi necessari per configurare davvero uno switch, gestendo le sue porte attraverso il sistema operativo con un accesso SSH.

UN INDIRIZZO IP PER LO SWITCH

Uno switch è un dispositivo di livello 2, quindi si occupa più che altro degli indirizzi MAC. Ma questo non significa che non possa anche usare gli indirizzi IP. Uno dei comandi più comodi è

```
show ip interface brief
```

è in un certo senso il corrispettivo di ifconfig sui sistemi GNU/Linux: mostra tutte le interfacce di rete. L'output dovrebbe essere qualcosa di questo tipo

```
Interface        IP-Address      OK?
Method Status        Protocol
FastEthernet0/1       unassigned
      YES manual down        down
FastEthernet0/2       unassigned
                 YES manual down
GigabitEthernet0/1       unassigned .
      YES manual down        down
GigabitEthernet0/2       unassigned
      YES manual down        down
Vlan1      unassigned        YES
 manual administratively down down
```

L'interfaccia Vlan1 è quella tramite cui si può raggiungere lo switch, per esempio per accedervi tramite telnet. Naturalmente, se questa interfaccia è disattivata (down) non possiamo assegnarle un IP e non possiamo collegarci allo switch da remoto. Per configurarla bisogna entrare nella modalità Privilege col comando

```
enable
```

e poi in Global configuration mode con

```
configure terminal
```

A questo punto si entra nella modalità di configurazione dell'interfaccia Vlan1 col comando

```
interface vlan1
```

Il prompt dovrebbe presentare la dicitura

```
Switch(config-if)#
```

A questo punto si può configurare l'interfaccia selezionata, per esempio assegnandole un indirizzo IP manuale, corredato da maschera di sottorete:

```
ip address 10.1.1.1 255.255.255.0
```

Ovviamente, la subnet mask è fondamentale. Come abbiamo visto nell'output del comando show ip interface brief, questa interfaccia è per opzione predefinita disabilitata a livello amministrativo (**administratively down**). Sostanzialmente, è un po' come quando su un sistema Linux si da il comando ifdown: l'interfaccia non è disabilitata a livello hardware, ma solo a livello software.

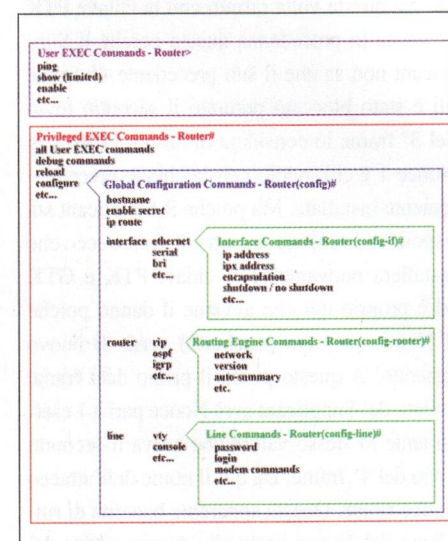



Fig. 1 • Le modalità di IOS sono una sorta di matrioska

Per abilitarla basta negare lo shutdown della porta, col comando

```
no shutdown
```

Otterremo una conferma del tipo

```
%LINK-5-CHANGED: Interface Vlan1,
        changed state to up
```

Se si vuole disabilitare nuovamente l'interfaccia, si deve dare il comando **shutdown**. È quindi abbastanza intuitivo: le varie interfacce fisiche non sono disabilitate, basta collegarsi con un cavo di rete e diventano **up**. Se se ne vuole disabilitare una, basta ordinare il suo shutdown. Se poi si vuole riabilitare, si specifica "no shutdown". L'interfaccia Vlan1 funziona al contrario, essendo disabilitata per opzione predefinita per ovvi motivi di sicurezza. Se controlliamo nuovamente le interfacce con

```
do show ip interface brief
```

Otterremo

```
Interface        IP-Address      OK?
        Method Status        Protocol
FastEthernet0/1          unassigned
          YES manual down        down
FastEthernet0/2          unassigned
                    YES manual down
GigabitEthernet0/1       unassigned
          YES manual down        down
GigabitEthernet0/2       unassigned
          YES manual down        down
Vlan1       10.1.1.1     YES manual
                        up       down
```

Come si può notare, adesso Vlan1 risulta attiva (manual up), anche se con protocol down perché al momento non vi è alcun traffico sulla porta (nessuno è connesso). Per poter vedere l'elenco delle interfacce è stato necessario premettere **do** al comando, perché ci si trova nella modalità di configurazione dell'interfaccia, e il comando appartiene alla modalità priviledge exec mode.

UNA RETE PRIMITIVA

Nella prove che abbiamo fatto finora con PacketTracer non abbiamo una rete a disposizione, solo un semplice switch. Per avere almeno una rete locale minimale dobbiamo aggiungere un secondo dispositivo, un **End Device**. Per esempio, un semplice **PC**. Dopo averlo aggiunto bisogna connetterlo allo switch. La soluzione più semplice consiste nell'andare nella barra degli strumenti, sezione **Connections**, e selezionare l'icona col fulmine, cioè **Automatically choose connection type**, collegando i due dispositivi. Nella schermata della console (CLI) dello switch noteremo apparire le righe

```
%LINK-5-CHANGED: Interface Fast
  Ethernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol
     on Interface FastEthernet0/1,
  changed state to up %LINEPROTO-5-
UPDOWN: Line protocol on Interface
        Vlan1, changed state to up
```

L'ultima riga indica che il computer è stato connesso all'interfaccia **Vlan1**. Quelle precedenti, invece, ci comunicano che la porta fisica utilizzata per la connessione è **FastEthernet0/1**.
Naturalmente, anche il PC va configurato: con un doppio click su di esso accediamo alla scheda **Config** e poi all'interfaccia **FastEthernet0**. Qui possiamo stabilire una configurazione IP statica, con indirizzo **10.1.1.2** e subnet mask **255.255.255.0**. Ci possiamo subito spostare nella scheda **Desktop**, per avviare un **command prompt**. Questo simula il prompt dei comandi di Windows. Purtroppo non è disponibile la simulazione del terminale bash ma poco importa: per ora ci interessa soltanto un ping verso lo switch. Possiamo inviare i pacchetto ICMP con il comando

```
ping 10.1.1.1
```

Se abbiamo configurato correttamente la Vlan1 dello switch dovremmo ottenere una risposta di questo tipo:

```
Pinging 10.1.1.1 with 32 bytes
                          of data:
Reply from 10.1.1.1: bytes=32
                  time<1ms TTL=255
Reply from 10.1.1.1: bytes=32
                  time<1ms TTL=255
Reply from 10.1.1.1: bytes=32
                  time<1ms TTL=255
Reply from 10.1.1.1: bytes=32
                  time<1ms TTL=255
Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4,
               Lost = 0 (0% loss),
Approximate round trip times in
                     milli-seconds:
    Minimum = 0ms, Maximum = 0ms,
                      Average = 0ms
```

Se lo switch risponde almeno alle ultime richieste, perché le prime potrebbero andare in timeout vista la necessità di rilevare il MAC dello switch tramite pacchetti ARP, significa che possiamo configurare il dispositivo tramite telnet. Basta, dal prompt del computer, dare il comando

```
telnet 10.1.1.1
```

e accedere alla console dello switch, usando la password che avevamo impostato precedentemente. Ci troviamo in una simulazione, ed è esattamente come se nel mondo reale stessimo cercando di connetterci da un computer allo switch per configurarlo senza bisogno di un accesso fisico diretto. Da notare che mentre dalla console fisica dello switch è sempre possibile dare il comando **enable**, da telnet non è possibile a meno che non sia stata indicata una password. La password per il comando enable è sostanzialmente come la password di sudo sui sistemi Linux, protegge l'esecuzione del comando per ottenere i privilegi di amministrazione. Per impostarla bisogna accedere alla console fisica dello switch e digitare

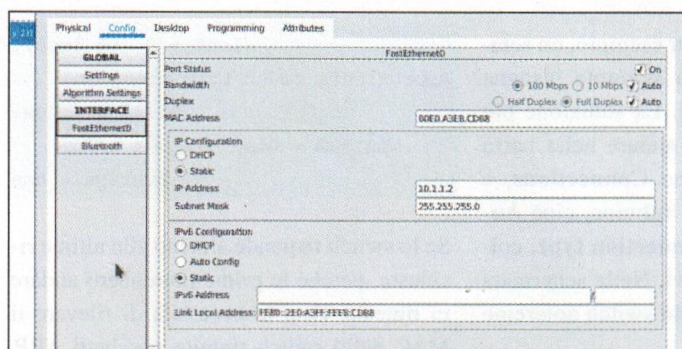
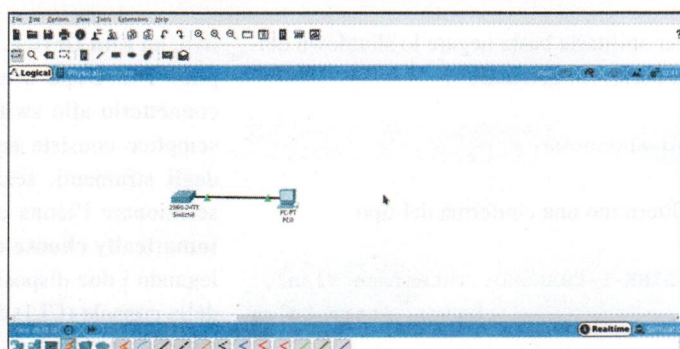
```
enable password nuovapassword
```

Solo a questo punto si potrà dare il comando enable, inserire la password, e ottenere la privilege mode da telnet. La configurazione può poi essere salvata col comando

```
write
```

che deve essere dato dalla modalità privilege exec mode. Se si stavano eseguendo delle configurazioni probabilmente ci si trova in una modalità di configurazione: il modo più rapido per tornare indietro e raggiungere la modalità privilege è premere **Ctrl+X**. Esiste anche un altro metodo per salvare la configurazione, che è generalmente consigliato da Cisco. Bisogna dare il comando

```
copy running-config startup-config
```

Il primo argomento è l'origine, il secondo

■ **Fig. 2 • Tramite la scheda Config è facile configurare un nuovo dispositivo in PacketTracer**

■ **Fig. 3 • Una rete molto semplice costituita da uno switch e un PC**

la destinazione: con questo comando stiamo dicendo che vogliamo copiare la configurazione attualmente attiva nella posizione della configurazione che viene caricata all'avvio del dispositivo. Così non perderemo le modifiche al riavvio.
Il comando copy è effettivamente molto più versatile, perché permette di leggere e scrivere la configurazione da vari punti, per esempio anche da TFTP o da un file in memoria flash.

TELNET È OBSOLETO

Finora abbiamo menzionato Telnet, ma questa tecnologia ha un problema notevole: il traffico non è crittografato. E non è una buona idea inviare le password di amministrazione di uno switch o router in chiaro su una rete, considerando che alcuni malintenzionati potrebbero sniffare il traffico e scoprire la password. Per fortuna, è possibile usare SSH, che utilizza una crittografia a doppia chiave per garantire la riservatezza della comunicazione. Per abilitare SSH, però, bisogna eseguire una serie di operazioni preliminari. Prima di tutto (nella modalità **configure global**) si devono impostare sia l'hostname che il nome di dominio:

```
hostname ilmioswitch
ip domain-name lamiaazienda.it
```

Il nome di dominio può essere uno qualsiasi, non deve necessariamente esistere come nome registrato su internet (anche perché è possibile non essere nemmeno connessi a internet). Si deve poi creare la chiave segreta, come si fa sui sistemi GNU/Linux col comando ssh-keygen. Su Cisco IOS si deve utilizzare il comando

```
crypto key generate rsa
```

Ci fornirà questo tipo di output:

```
The name for the keys will be:
                    switch1.lamiaazienda.it
Choose the size of the key modulus
  in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a
 key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
```

Chiedendo quindi quanti bit usare per la chiave. La dimensione predefinita è 512 bit, ma è un po' troppo piccola. Meglio salire almeno a 1024 bit, per ridurre il rischio che qualcuno possa forzarla.
Ora che la coppia di chiavi, pubblica e privata, è stata creata, possiamo tranquillamente abilitare il "demone" SSH con il comando

```
ip ssh version 2
```

Nello specifico, questo comando abilita SSH con la seconda versione del protocollo. Ora dobbiamo indicare almeno un utente con la propria password: un vantaggio di SSH è di poter creare diversi utenti, ciascuno con una propria password. Il comando username permette di indicare questi due dati:

```
username ted password alligatore3
login local
```

Il comando **login local** costringe il sistema a rifiutare una eventuale password geenrale (quella che viene impostata per Telnet), e pretendere invece l'autenticazione tramite i vari nomi utenti e le relative password. Questo è comodo quando la rete va gestita da diverse persone, e si suppone che prima o poi sarà necessario revocare l'accesso ad alcuni amministratori. Se con telnet tutti usano la stessa password, con SSH ogni utenti può avere una password diversa. Per abilitare le connessioni SSH bisogna poi configurare nello specifico le linee vty, perché sono le stesse usate per il controllo remoto anche con Telnet.

```
line vty 0 15
```

Se diamo il comando

```
transport input ?
```

Vediamo la lista delle varie modalità con cui possiamo permettere l'accesso ai terminali remoti:

```
  all     All protocols
  none    No protocols
  ssh     TCP/IP SSH protocol
  telnet  TCP/IP Telnet protocol
```

Siccome è una buona idea disabilitare Telnet, possiamo indicare semplicemente

```
transport input ssh
```

In questo modo verranno accettate solo connessioni SSH provenienti da altri dispositivi.

LE PORTE DI UNO SWITCH

Uno switch dispone di due modalità di funzionamento per le proprie porte: **access** e **trunk**. Selezionata una interfaccia, per esempio con

```
interface FastEthernet0/1
```

si può impostare la modalità con il comando

```
switchport mode access
```

oppure con

```
switchport mode trunk
```

La differenza sostanziale è che le porte di tipo Access sono dedicate ai vari end device, cioè i dispositivi degli utenti che si collegano alla nostra rete (PC, laptop, eccetera). Invece, le porte Trunk sono dedicate alla connessione di altri switch, cosa piuttosto comune per estendere la rete in altre stanze dell'edificio. La modalità Access è quella "normale", mentre la Trunk merita maggiore attenzione.
Quando il trunking è stabilito, i due switch si scambieranno il traffico, perché si prevede per l'appunto che siano da considerarsi come una sorta di uno switch, sdoppiato solo per convenienza fisica. Se abbiamo 4 PC in una stanza e altri 4 in quella accanto non ha senso far passare 4 cavi da una stanza all'altra con un unico switch, basta avere due distinti switch, uno per ogni stanza, e far passare un solo cavo da uno all'altro. Il Trunking può essere fatto usando il **Dynamic Trunking Protocol**, che è proprietario di Cisco. Secondo il DTP esistono tre diverse modalità di trunking:

- Desirable
- Auto
- No Negotiate

Si possono abilitare rispettivamente con i comandi

```
switchport mode dynamic desirable
switchport mode dynamic auto
switchport mode nonegotiate
```

Quando la porta è impostata come una **Desirable**, significa che considererà per opzione predefinita di essere connessa a dispositivi con cui fare trunking, cioè degli altri switch. Quindi, appena rileva che un dispositivo viene connesso alla porta, lo switch inizia a inviare pacchetti DTP per stabilire una connessione trunk tra i due switch. Se l'altro dispositivo è a sua volta in modalità Desirable oppure Auto, viene automaticamente stabilito il trunking. Se però entrambe i dispositivi sono in modalità Auto, non succede nulla: la modalità **Auto**, infatti, consiste semplicemente nell'aspettare che l'altro dispositivo prenda una decisione. Ovviamente, non è una buona idea lasciare tutte le porte di uno switch in modaltà Auto o Desirable se non è assolutamente necessario, perché un malintenzionato potrebbe scollegare un cavo e connettersi con un finto switch, sniffando tutto il traffico di rete. Per questo motivo esiste la modalità No Negotiate, che non utilizza DTP, ed è la modalità predefinita di tutte le porte.

Fig. 4 • La visualizzazione fisica aiuta a capire l'aspetto dei dispositivi

C'è da dire che nelle reti reali si usa comunque più di un cavo per colelgare due switch in un trunk: si usano almeno due cavi, con due porte in modalità trunk, per avere un backup. Usando un solo cavo c'è infatti il rischio di lasciare isolata una parte della rete se il cavo in questione dovesse essere danneggiato. Un secondo cavo può fungere da backup e salvare la connettività in caso di danneggiamento fisico del primo cavo.

LE FUNZIONI DI UNO SWITCH

Uno switch ha tre diverse funzioni principali:

- Address Learning
- Forwarding decision
- Loop Avoidance

L'**address learning** consiste nel memorizzare gli indirizzi MAC dei vari dispositivi connessi alle porte. In particolare, la **CAM table** è la tabella in cui uno switch memorizza l'indirizzo MAC di ogni dispositivo collegato a ciascuna delle sue porte. È importante, perché consente allo switch di sapere esattamente a quale porta sia connesso un determinato dispositivo. In questo modo, quando arriva un pacchetto destinato a un dispositivo è possibile inviarlo solo alla sua porta invece che a tutte le altre. Questo inoltro dei pacchetti al dispositivo destinatario è chiamato **Forwarding**, e lo switch può operare una scelta: cut through, oppure store&forward. Cut through significa che lo switch inoltrerà il pacchetto (il frame, visto che siamo sul livello datalink) al

IL GATEWAY

Al momento lo switch sta implementando solo una semplice rete locale, con un unico computer connesso, e non prevede alcuna possibilità di uscire su altre reti. Nella rete che abbiamo creato in effetti non ha senso, ma nel mondo reale si lavora anche con dei router, che fungono da gateway nella maggioranza dei casi. Per impostare un gateway principale sullo switch bisogna essere nella modalità di configurazione globale (quella a cui si accede con **configure terminal**), e utilizzare il comando per la configurazione IP:

```
ip default-gateway
                10.1.1.10
```

Dove ovviamente 10.1.1.10 è l'indirizzo del gateway.

destinatario così come gli arriva dall'origine, un bit dopo l'altro. Invece, col meccanismo store&forward lo switch aspetta di avere ricevuto tutto il pacchetto indirizzato al destinatario prima di inviarglielo. Ovviamente, la prima opzione è molto rapida, mentre la seconda è decisamente più affidabile (si riducono gli errori). La **Loop avoidance** è una caratteristica fondamentale per il funzionamento degli switch nelle reti complesse. Abbiamo infatti spiegato che in caso di trunking si collegano spesso almeno due cavi per eseguire il trunking, in modo da essere sicuri che non si perda la connessione quando qualcosa va storto con uno dei due cavi. C'è solo un problema: nella maggioranza dei casi i due cavi saranno perfettamente funzionanti contemporaneamente.

Questo significa che se il primo switch riceve da un PC un pacchetto di broadcast (che per definizione deve essere inviato a tutti i dispositivi della rete), si impegnerà a inviarlo a tutte le proprie porte, incluse quelle di trunking. Raggiunta la prima porta di trunking il pacchetto arriverà al secondo switch. Questo farà la stessa cosa, inviando il pacchetto su tutte le altre porte, e raggiungerà inevitabilmente la porta cui è connesso il secondo cavo di trunking. Il pacchetto tornerà quindi al primo switch, e ripeterà il percorso attraverso tutte le sue porte, entrando in un ciclo infinito. Il livello datalink non prevede nessun meccanismo di prevenzione dei loop, quindi gli switch devono "arrangiarsi". E lo fanno usando lo **Spanning Tree Protocol**. Si tratta di un semplice protocollo che permette agli switch di capire se ci siano dei collegamenti ridondanti, che portano agli stessi dispositivi. Nel caso del trunking con due cavi, quindi, gli switch si rendono

I QUIZ PRESENTI IN QUESTE PAGINA SONO ISPIRATI ALLE REALI DOMANDE CHE SI POSSONO TROVARE NELL'ESAME CISCO 200-125

I QUIZ

Domanda: Host A receives a frame and discards it after determining it is corrupt. Which OSI layer checks frames for errors?

A. Application
B. Network
C. Physical
D. Data-link
E. FCS or CRC.

Risposta: D. Infatti i frame sono i pacchetti di livello datalink: nonostante questo livello non possieda un vero e proprio controllo di sessione, dispone della Frame Check Sequence per verificare l'integrità dei pacchetti. Naturalmente, il controllo dei frame non può essere fatto da nessun altro livello, quindi anche per esclusione è ovvio che solo sul livello datalink si possono controllare i pacchetti datalink.

Domanda: No matter how it's configured, a single switch port is considered what?

A. A separate unicast domain
B. A separate broadcast domain
C. A separate multicast domain
D. A separate collision domain

Risposta: D. Diversamente da un hub, nel quale tutti i dispositivi fanno parte di un unico collision domain, in uno switch ogni porta ha un proprio collision domain. Si tratta di una caratteristica hardware, che non può essere cambiata con la configurazione dello switch.

Domanda: Which of the following is the correct syntax to configure a switch port as a standard user port on VLAN 10 for data and VLAN 50 for VoIP?

A. SW1(config-if)#switchport mode trunk
   SW1(config-if)#switchport access vlan 10
   SW1(config-if)#switchport voice vlan 50
B. SW1(config-if)#switchport mode access
   SW1(config-if)#switchport access vlan 10
   SW1(config-if)#switchport voice vlan 50
C. SW1(config-if)#switchport mode trunk
   SW1(config-if)#switchport access vlan 10
   SW1(config-if)#switchport voip vlan 50
D. SW1(config-if)#switchport mode access
   SW1(config-if)#switchport access vlan 10
   SW1(config-if)#switchport voip vlan 50
E. SW1(config-if)#switchport mode access
   SW1(config-if)#switchport access vlan 50
   SW1(config-if)#switchport voice vlan 10

Risposta: B. Per poter essere usata dagli utenti, la porta deve essere in modalità access invece che in modalità trunk. La porta da usare per i dati (nell'esempio al vlan10) rimane come access, mentre l'altra può essere indicata come voice (la modalità voip non esiste, il nome giusto è voice).

Domanda: Which Ethernet switching method would you use if low latency is of utmost importance?

A. First-in-first-out
B. Store-and-forward
C. Cut-through
D. Cisco Express Forwarding (CEF)
E. Queuing

conto che il secondo cavo è ridondante, e lo disabilitano a livello logico: il cavo è ancora connesso fisicamente, e nel caso serva un backup le porte ethernet a cui è connesso verranno riattivate. Ma finché il primo cavo resiste si userà soltanto quello per eseguire il trunking.

PACKETTRACER: STRUTTURA LOGICA E FISICA

Osservando l'interfaccia di PacketTracer ci si accorge subito che offre due modalità di visualizzazione: **Logical** e **Physical**. La vista logica ci permette di collegare i vari dispositivi a livello concettuale, per stabilire come siano costruite le varie reti: un paio di computer possono essere collegati a uno switch, il quale è poi connesso a un router, e questo a sua volta è connesso a altri dispositivi. Questa modalità ci permette di creare tutte le reti che vogliamo e collegarle come preferiamo. C'è solo un problema: nel mondo reale le cose non sono proprio così semplici. I dispositivi devono infatti avere una posizione fisica, e spesso sono distanti fra loro. In una azienda è perfettamente plausibile che dispositivi della stessa rete locale debbano essere posizionati in stanze o piani diversi di un edificio. E che invece una grande stanza debba contenere dispositivi appartenenti a reti diverse. Oltre al fatto che spesso si devono collegare dispositivi in edifici separati, magari anche abbastanza lontani. La visualizzazione fisica ci permette di fare proprio questo, simulare la distribuzione dei vari dispositivi di rete in diversi ambienti. E anche di prendere confidenza con l'aspetto fisico delle reti, seppure nei limiti di una simulazione.

Risposta: C. La modalità più rapida per l'inoltro dei frame è cut-through, nella quale i bit vengono inoltrati immediatamente. Invece, in store-and-forward i bit vengono raccolti finché il frame è completo, e solo a quel punto inoltrati alla porta del destinatario.

Domanda: You need to verify the MAC address of FastEthernet0/1 on your Cisco IOS. Which command will display the MAC address?

A. show interfaces FastEthernet0/1
B. show mac-address-table
C. show ip route
D. show version
E. show ip interface brief
F. show running-config

Risposta: B. Il comando che abbiamo già visto, show ip interface brief, mostra solo le informazioni relative agli IP, non ai MAC. Per leggere gli indirizzi MAC abbiamo bisogno dell'apposita tabella, che possiamo leggere per intero col comando show mac-address-table. Ricordiamo che basta scrivere show ? per avere l'elenco delle varie tabelle che si possono leggere, e quella dei MAC risalta chiaramente. A dirla tutta, se si è interessati solo a una singola porta si può estrarre l'informazione col comando show mac-address-table interfaces FastEthernet 0/1.

Domanda: Your manager has requested you indicate which of the above ports will be Spanning Tree Protocol-designated ports.

A. Switch V1, Port Fa0/0; Switch V3, Port Fa0/0; Switch V3, Port Fa0/24
B. Switch V1, Port Fa0/24; Switch V2, Port Fa0/0; Switch V2, Port Fa0/24

Risposta: B. In una situazione simmetrica come questa, tutte le strade sembrano egualmente valide. Ovviamente, il protocollo STP prevede un metodo per prendere comunque una decisione. E si basa sul Bridge ID, un identificativo univoco di ogni dispositivo composto da 8 byte. I primi 2 byte rappresentano la priorità, mentre gli ultimi 6 byte sono semplicemente l'indirizzo MAC di ogni dispositivo. Il dispositivo col BridgeID più basso è il root, e quindi è quello che "prende tutto". In questo caso, la priorità di tutti i dispositivi è uguale, quindi è irrilevante. Ci interessa solo il MAC, e il più basso (come numero esadecimale) è chiaramente quello di V2. Segue V1, e il più alto di tutti è il MAC di V3. Le due porte di V2 saranno quindi entrambe usate dal protocollo STP, mentre per il dispositivo V1 verrà tenuta in considerazione solo la porta che dialoga con l'altro dispositivo. Le porte di V3 non saranno utilizzate (STP le mette nello stato Blocking per evitare un loop), perché ha il MAC più alto.

Domanda: Refer to the following configuration:

```
line vty 0 4-
password 98702204
login
transport input ssh
```

What is the effect?

A. It configures SSH globally for all logins with local users.
B. It tells the router or switch to try to establish an SSH connection first and if that fails to use Telnet.
C. It configures the virtual terminal lines with the Telnet password 98702204.
D. It configures a Cisco network device to use the SSH protocol on incoming communications via the virtual terminal ports.
E. It allows seven failed login attempts before the VTY lines are temporarily shutdown.

Risposta:D. Con questa configurazione è permesso solo l'accesso tramite SSH, per avere anche Telnet si dovrebbe impostare all come protocollo. Attenzione, però: non bisogna pensare che si entri in SSH tramite la propria password utente. Dando solo il comando login invece di login local tutti useranno la stessa password di accesso.

IL REGISTRATORE DI CASSA OPEN SOURCE

Si chiama IoTPOS ed è il software progettato per Raspberry Pi che ti consente di dare un tocco di classe e innovazione alla tua attività commerciale. Ecco come installarlo e configurarlo

Mettere in piedi una nuova attività imprenditoriale può essere complicato, non solo per la burocrazia necessaria per intraprendere una nuova avventura, ma anche per gestire le vendite e gli incassi. Il registratore di cassa è uno strumento fondamentale, ma spesso costoso e poco pratico da utilizzare. Per semplificare la vita dei commercianti e per ridurre i loro costi esiste **iotPOS**: si tratta di un programma progettato appositamente per i Rasperry Pi (qualsiasi modello in circolazione, dal più "vecchio" 1 al più recente 3), i mini computer dal basso costo d'acquisto (meno di 50 euro) e dall'altrettanto irrisorio consumo energetico (aspetto, questo, da non sottovalutare quando si avvia una nuova attività commerciale). Grazie ad un Raspberry Pi ed al software iotPOS possiamo quindi realizzare un proprio registratore di cassa moderno e funzionale, che non ha nulla da invidiare ai modelli più "commerciali" (e spesso closed) in circolazione. Anzi, sono questi ultimi a dover invidiare qualcosa a iotPOS.

COSA OFFRE IOTPOS?

Il software non solo aiuta aiuta il commerciante permettendogli di fare un inventario e di ottenere immediatamente le statistiche sulla merce venduta, ma offre anche la possibilità di realizzare delle casse automatiche, nelle quali i clienti possano scansionare gli articoli ed ottenere il conto da pagare. Una funzionalità già utilizzata in diversi ristoranti, così come in diverse attività commerciali fuori dall'Italia (nel Regno Unito, ad esempio, molti supermarket offrono casse automatiche che riducono al minimo le lunghe file alle casse alle quali, purtroppo, in Italia siamo abituati). Questo programma risulta particolarmente utile se abbinato ai moderni lettori di carte di credito a basse commissioni, che permettono ormai a qualsiasi commerciante di accettare pagamenti tramite carte di credito, di debito, o addirittura account PayPal senza dover pagare commissioni enormi. Soprattutto perché essendo calcolate in percentuale è possibile fare pagamenti anche di pochi centesimi. Uno di questi servizi/dispositivi è, ad esempio, SumUp (***https://sumup.it/***).

INSTALLIAMO IL NECESSARIO

Installare IoTPOS su un Raspberry Pi richiede alcuni passaggi per nulla complicati. In particolare, è necessario compilare il software e configurare il sistema affinché tutto possa funzionare al meglio. Per facilitare il processo di installazione, abbiamo deciso di realizzare uno script che automatizza il processo di automazione. Per lanciarlo, basta accedere al terminale del sistema operativo installato sul nostro Raspberry Pi (ad esempio Raspbian) e da qui lanciare i seguenti comandi:

```
wget -o iotPOS_install.sh https:
        //pastebin.com/raw/Mj39sfDV
dos2unix iotPOS_install.sh
chmod +x iotPOS_install.sh
./iotPOS_install.sh
```

Lo script richiede soltanto di inserire le credenziali del proprio Google Account. Più nel dettaglio, questo dato è fondamentale per consentire ad IoTPOS di utilizzare GMail, in modo da poter utilizzare l'invio di email.
Ovviamente il Raspberry Pi deve essere collegato ad una stampante di scontrini, in modo da fornire all'utente finale una ricevuta d'acquisto. Ne esiste una prodotta da **Adafruit**, che si può trovare sul Web cercando "*thermal receipt printer*", e che costa meno di 40 euro. La stampante va collegata soltanto ai

Fig. 1 • Corredato di una stampante termica, il software IoTPOS si dimostra come una soluzione professionale ed innovativa in concorrenza con tutti i "classici" registratori di cassa

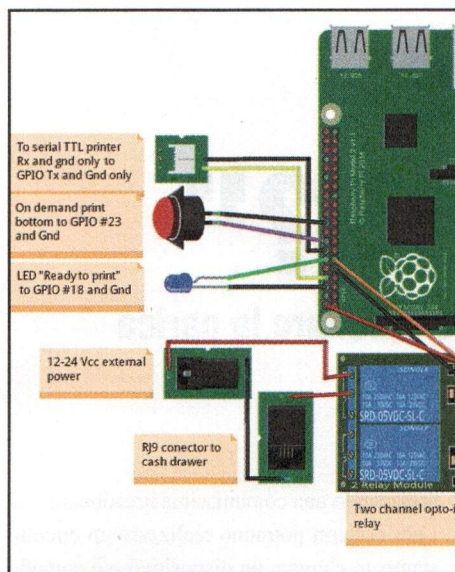



Fig. 2 • Ecco lo schema di collegamento del Raspberry Pi con gli altri componenti

Fig. 3 • L'interfaccia grafica di IoTPOS è semplice e intuitiva, anche grazie alla presenza di immagini che permettono di identificare più velocemente i prodotti

pin **GND** e **Tx** del Raspberry Pi, come si vede nello schema in **Fig. 2**. Per rendere il tutto più completo e simile ad un classico registratore di cassa, si può poi aggiungere un relay che gestisce l'apertura del cassetto per inserire il denaro incassato.

CONFIGURAZIONE IN CORSO

Per cominciare a configurare il proprio registratore di cassa basta lanciare da terminale il comando **iotstock** ed utilizzare le credenziali di accesso predefinite: **admin** e **linux**, rispettivamente come username e password. Ovviamente, per garantire un grado più elevato di sicurezza, possono essere modificate in seguito. L'interfaccia (**Fig. 3**) è costruita a schede e permette di aggiungere nuovi prodotti all'interno del negozio.
La scheda **Products** permette di gestire i prodotti del proprio negozio, mentre **Quick Plots** (**Fig. 4**) offre grafici che indicano quali merci vengano vendute più spesso: un'ottima visione che ci permette di capire quali siano i prodotti più in voga e quelli che forse è meglio evitare di continuare a vendere perché non apprezzati dai clienti.
Quando si crea un prodotto è anche possibile stampare il suo codice a barre, con la stessa stampante per gli scontrini, così da applicarlo sulla confezione del prodotto stesso.

Nel caso in cui volessimo consentire agli utenti di pagare autonomamente, dunque creare una cassa automatica, collegando il Raspberry Pi ad uno schermo touch si può offrire ai propri clienti un'interfaccia utente molto semplice. L'interfaccia si apre lanciando il programma IoTPOS, e presenta i vari prodotti corredate da immagini esplicative (consentendo dunque una rapida individuazione del prodotto da "scontrinare"). Per scegliere un prodotto basta cercarlo nell'elenco, oppure scrivendo il nome nella barra di ricerca, e cliccarci sopra (o toccandolo, se con è presente uno schermo touchscreen). Si può anche usare un qualsiasi lettore di codici a barre USB per scansionare il codice a barre (stampato, come abbiamo già consigliato in precedenza).
Alla fine, il dispositivo stampa uno scontrino, che può essere consegnato all'utente. Naturalmente, per quanto riguarda il venditore, il programma mantiene tutta la contabilità, quindi nel caso di controlli fiscali è sufficiente offrire i tabulati delle vendite.

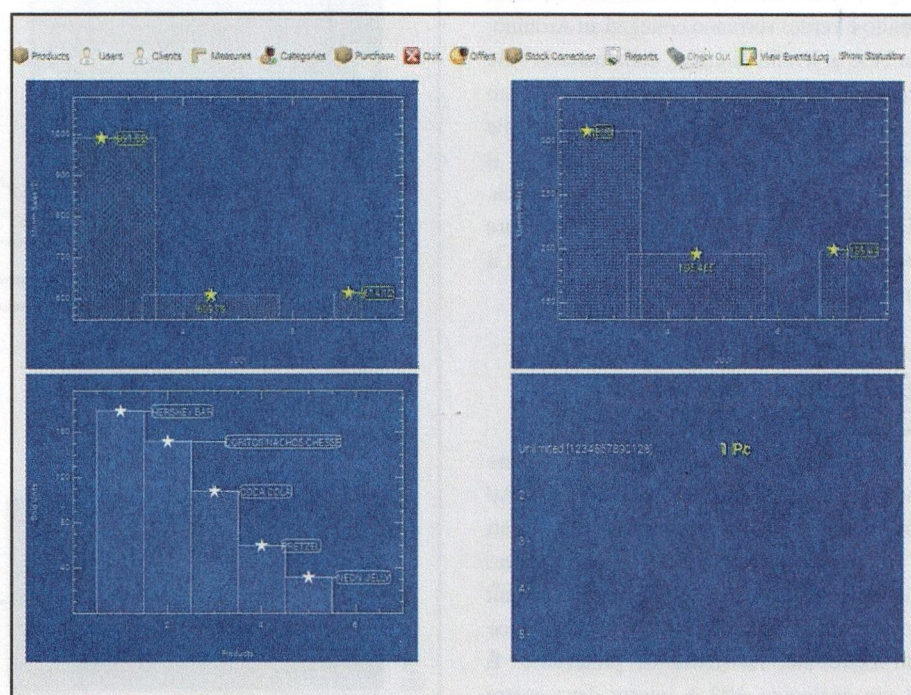



Fig. 4 • Con la funzionalità Quick Plots è possibile ottenere le statistiche di vendita

"QUANT'È CARICA QUELLA BATTERIA?"

Realizziamo con Arduino un sistema che ci permette di controllare la carica di qualsiasi batteria. Con il nostro aiuto è tutto più semplice!

Le batterie alcaline sono probabilmente l'oggetto più acquistato di tutti i tempi: telecomandi, orologi, radio FM portatili, giocattoli hanno tutti bisogno di un po' di energia per poter funzionare correttamente. Fortunatamente, però, esistono anche delle versioni ricaricabili che, a differenza delle usa e getta, sono sempre più utilizzare. Ma se volessimo monitorare lo stato di carica di una qualsiasi batteria stilo? In commercio esistono dei dispositivi che ci permettono di farlo. Ma, da veri maker, possiamo realizzarne uno in casa a costo zero, a patto di avere, ovviamente, una scheda Arduino. Oltre alla scheda di prototipazione, infatti, ci occorrono solo una manciata di LED e resistenze: Arduino a parte, una spesa che si riduce a qualche centesimo di euro. Il progetto che realizzeremo è abbastanza semplice: come si può notare dallo schema in Fig. 1, 3 LED di differente colorazione (rosso, giallo e verde) verranno collegati ad Arduino; in base al livello di carica della batteria stilo collegata al circuito si accenderà il giusto LED (rosso se scarica, verde se carica, gialla se mediamente carica). Ma è arrivato il momento di passare dalla teoria alla pratica. Tuffiamoci subito in questa nuova avventura e scopriamo in anticipo se sta per arrivare il momento di cambiare le batterie!

SCHEMA DI COLLEGAMENTO

I pin di Arduino da utilizzare sono, almeno nel nostro test, 8, 9 e 10, fra i digitali, e A0 fra gli analogici. Ai primi 3 vanno collegati i LED di cui abbiamo parlato in precedenza: ricordiamoci che, al fine di evitare eventuali guasti sui LED utilizzati, è sempre bene utilizzare una resistenza di protezione. E il pin analogico A0? A questo deve essere collegato il positivo della batteria da verificare: l'ATMega328 dell'Arduino, in base al nostro sketch, si occuperà di convertire il segnale analogico (i Volt della batteria) in digitale facendo accendere poi il giusto LED. Tra il positivo della batteria e il pin A0, però, è necessario porre una resistenza da 10 kOhm. A cosa serve? In gergo tecnico, questo resistore viene detto di pull-down ed ha uno scopo importante: quello di eliminare eventuali disturbi provenienti dalla batteria. È dunque evidente, al fine di ottenere una valutazione corretta della carica della batteria stilo, come sia importante non sottovalutare il collegamento di tale resistore.

Come già anticipato, lo schema di collegamento è evidentemente molto semplice: proprio per la sua semplicità possiamo prototipare il tutto in pochi secondi utilizzando una comunissima breadboard; ma i più esigenti potranno realizzare un circuito stampato e creare un dispositivo più comodo da utilizzare o portare in giro ogniqualvolta ce ne sarà bisogno.

LO SKETCH

Chiunque abbia già sviluppato qualcosa con Arduino, saprà già che la prima cosa da fare è la dichiarazione delle variabili:

```
int carica;
int Rosso=8;
int Giallo=9;
int Verde=10;
```

Anzitutto ne creiamo una che ci tornerà

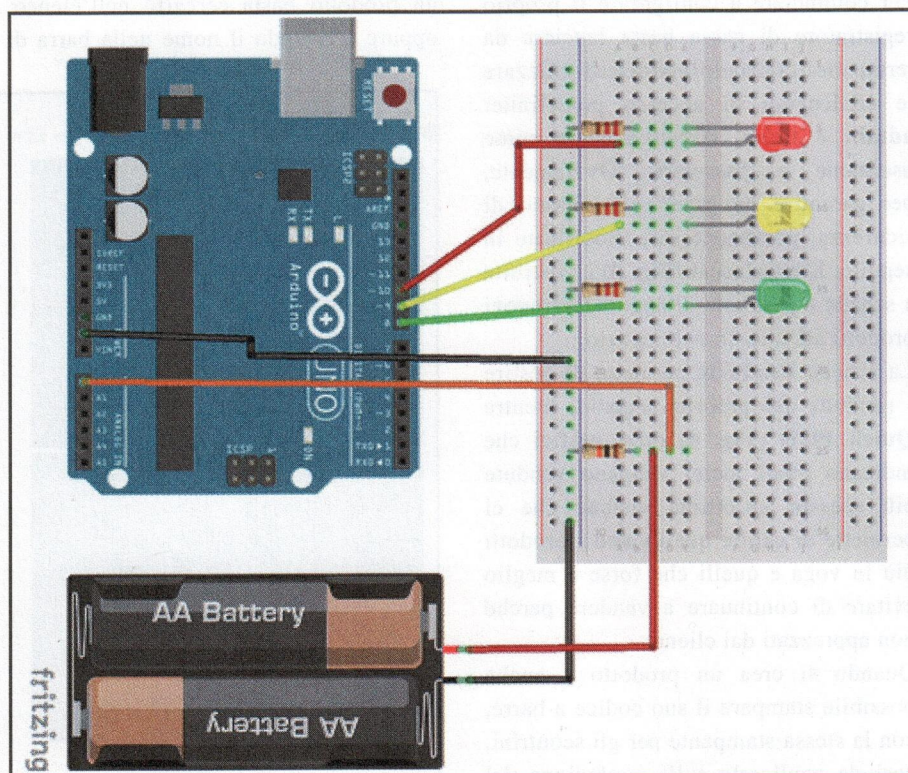



Fig. 1 • Ecco lo schema di collegamento su breadboard

utile per memorizzare il valore analogico convertito in digitale. Poi, ovviamente, dichiariamo 3 differenti variabili che identificano i corrispondenti 3 LED collegati ad Arduino. Queste ultime 3 variabili devono essere poi dichiarate come uscite, dunque:

```
void setup()
 {
  pinMode(8,OUTPUT);
  pinMode(9,OUTPUT);
  pinMode(10,OUTPUT);
 }
```

Ma ritorniamo un secondo alla variabile carica dichiarata ad apertura dello sketch. Abbiamo già detto che ci servirà per memorizzare un valore convertito da analogico a digitale. I più informati sapranno già che Arduino lavora a 5 V. Di conseguenza, riusciremo a leggere solo i valori compresi tra 0 e 5 V. Traducendo ciò in bit, riusciremo a leggere tutti i valori che vanno da 0 (0 V) a 1023 (5 V). Se la batteria (o le batterie) da verificare hanno una tensione massima di 5 V è tutto semplice. Ma se volessimo controllare una stilo da 1,5 V ad esempio? Basta un semplice calcolo matematico: dividiamo 1023 per 5 V e moltiplichiamo il risultato ottento per i Volt della batteria.
Dunque, sempre nel caso di una batteria da 1,5 V, la tensione massima equivarrà ad un valore pari a 307. Teniamo ben a mente questa semplice formula matematica perché a breve ci servirà per personalizzare il codice dello sketch a seconda delle nostre esigenze.

```
void loop()
{
 delay(100);
 carica=analogRead(0);
 if (carica>265)
   {
     digitalWrite(Rosso,LOW);
     digitalWrite(Giallo,LOW);
     digitalWrite(Verde,HIGH);
   }
```

Diciamo ad Arduino di andare a leggere il valore (analogico) al pin A0, che corrisponde alla variabile carica precedentemente dichiarata. Se questo valore è superiore a 265 allora il LED di colore verde si accenderà per indicare che la batteria è carica. Ma a cosa corrisponde

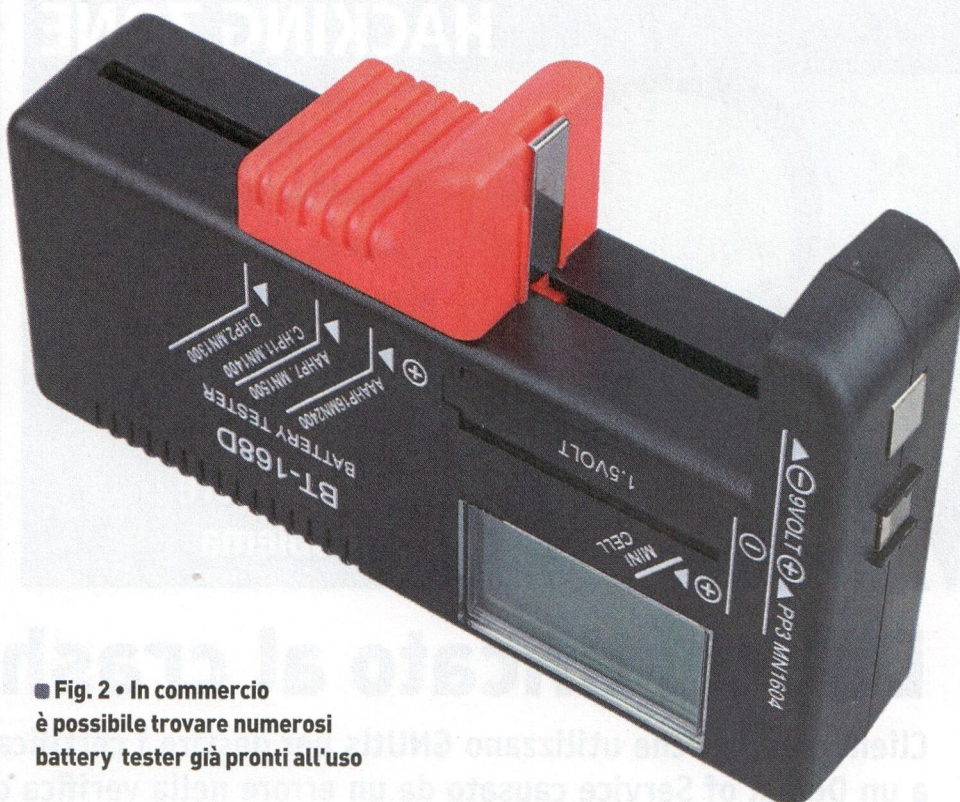



Fig. 2 • In commercio è possibile trovare numerosi battery tester già pronti all'uso

265? Nel caso del test di una batteria da 1,5 V corrisponde al valore convertito di 1,3 V, un valore ancora sufficiente per far sì che la batteria utilizzata nei nostri test venga considerata carica.

```
if ((carica<265)&&(carica >=164))
  {
    digitalWrite(Rosso,LOW);
    digitalWrite(Giallo,HIGH);
    digitalWrite(Verde,LOW);
  }
```

Analogamente al ciclo utilizzato per verificare la carica completa della batteria, nel caso in cui il valore letto al pin A0 e memorizzato nella variabile carica abbia un valore compreso tra 265 e 164 (ovvero 1,3 V e 0,8 V), facciamo sì che si accenda il solo LED giallo ad indicare una carica media e dunque una sostituzione quasi imminente della batteria.

```
if (carica<164)
  {
    digitalWrite(Rosso,HIGH);
    digitalWrite(Giallo,LOW);
    digitalWrite(Verde,LOW);
  }
```

Infine, se il valore rilevato è inferiore a 164 (come già detto, 0,8 V) accendiamo il LED rosso ad indicare che la carica della batteria collegata è troppo bassa e che è certamente il caso di procedere alla sostituzione o, se possibile, alla ricarica.

CONCLUSIONI

Come abbiamo avuto modo di scoprire, questo progetto Arduino è semplice non solo dal punto di vista dei collegamenti, ma anche lato codice. Alla fine, infatti, si tratta di 3 semplici cicli che, in base al valore rilevato, consentono di accendere il giusto LED. L'unica difficoltà, se così vogliamo definirla, sta nel tarare lo sketch a seconda delle proprie esigenze. Utilizzando il codice di test, infatti, è possibile ottenere un risultato esatto solo nel caso in cui venga collegata una batteria stilo da 1,5 V. Resta ovvio, dunque, che è il caso di cambiare i valori della variabile carica a seconda della batteria (o delle batterie) che vogliamo verificare. I più audaci potranno però espandere questo progetto che, come sempre, è solo un punto di partenza: si può infatti pensare di collegare diversi pulsanti ad Arduino che attivano diversi "profili": ad ogni profilo corrisponde una diversa batteria (da 1,5 e da 3 V ad esempio) in modo tale da evitare di mett ere mano al codice ogniqualvolta vorremo verificare batterie che hanno tensioni dichiarate differenti.

HACKING ZONE

Su ogni numero trovi l'analisi dettagliata delle vulnerabilità più pericolose e le soluzioni più adatte per risolvere il problema

Dal certificato al crash

Client e server che utilizzano GNUtls per gestire i certificati SSL/TLS sono vulnerabili a un Denial of Service causato da un errore nella verifica dei dati. Con un certificato contraffatto è possibile mandare in crash la libreria e disattivare il server

Uno dei meccanismi più comuni per garantire una comunicazione sicura tra due dispositivi è la crittografia a doppia chiave. Ciascuno degli interlocutori ha una chiave pubblica, che tutti possono usare per crittografare cioè che vogliono inviargli, e una chiave privata, che può usare soltanto lui per decifrare il contenuto dei messaggi. Esistono vari strumenti che implementano questo tipo di crittografia sui sistemi Unix: i principali sono OpenSSL e GNUtls. Il più usato è sicuramente OpenSSL, ma anche GNUtls è richiesto da molte applicazioni di uso comune. Quando viene utilizzato per gestire le connessioni SSL/TLS, come nel caso del protocollo HTTPS, segue le specifiche dello standard X.509. Quando si visita un sito web, soprattutto un sito che deve essere molto sicuro (come quello della propria banca), il sito web invia il proprio certificato (la chiave pubblica) al browser web, e viceversa. Il certificato è solitamente un file con estensione pem, che deve essere verificato per assicurarsi che provenga davvero dal server web. Altrimenti un qualsiasi pirata potrebbe creare un certificato finto e spacciarsi per uno dei principali istituti bancari. La verifica avviene in due passaggi: in primo luogo, il browser controlla presso una Certificate Authority che il certificato crittografico ricevuto appartenga davvero al sito che si è presentato con tale certificato. Ogni CA ha semplicemente una lista di nomi di dominio e altre informazioni con associate le chiavi pubbliche (chiamata trust list, lista di fiducia), quindi basta cercare il nome di dominio e vedere se la chiave pubblica fornita dal sito sia la stessa assegnata al suo nome di dominio. Poi, si invia al server un testo crittografato con la chiave pubblica: se questo riesce a decifrarla e rispedirla al browser vuol dire che è davvero chi sostiene di essere, perché solo il legittimo proprietario della chiave pubblica possiede anche la chiave privata necessaria a decifrare il testo.

■ **Fig. 1 • Un certificato contraffatto manda in crash GNUtls, e ogni programma che dipende da questa libreria**

IL PUNTATORE È LIBERO, I DATI NO

In GNUTLS, la verifica di un certificato viene operata da una serie di funzioni, riconducibili alla funzione gnutls_x509_trust_list_verify_crt(). Nel 2017 la funzione venne modificata per correggere un piccolo difetto. Le righe finali passarono da:

```
cleanup:
  return result;
```

alla versione:

```
cleanup:
  gnutls_free(signature->data);
  return result;
```

Questo piccolo bugfix serviva a tamponare un memory leak non particolarmente grave, ma che ovviamente doveva essere risolto. Con l'uso della funzione **gnutls_free** la memoria viene effettivamente liberata. C'è però un problema: scrivendolo così, l'unica cosa che avviene è che il puntatore all'area di memoria viene liberato, ma i dati non vengono cancellati. La differenza è importante, perché in questo modo i programmi multi-thread che usano la libreria si ritrovano in una situazione di use-after-free, cioè con altre funzioni che usano ancora i dati nonostante il puntatore sia stato liberato. Si tratta di un accesso "illegale", che provoca il crash della libreria e solitamente anche del programma che ne sta facendo uso. Nei programmi a singolo thread si verifica un double-free, con un secondo tentativo di liberare il puntatore ai dati (che però è già stato liberato in precedenza), risultando sempre in un crash.

L'EXPLOIT

Ci si potrebbe chiedere: ma se il tentativo di verifica di un certificato, operazione molto comune, manda in crash il programma come è possibile che nessuno se ne sia accorto prima? Il fatto è che il problema non si presenta in tutti i casi. Anzi: per renderlo evidente serve un certificato malevolo, creato appositamente per innescare il bug. In particolare, devono essere impostati dei parametri errati. Un file pem, infatti, è un certificato codificato in base64. Il certificato non contiene soltanto la chiave crittografica pubblica, che è comunque l'informazione più importante, ma anche una serie di altre informazioni. Questo servono per facilitare la verifica del certificato, e vengono quindi usate da programmi come OpenSSL o GNUtls. Un modo per leggerle facilmente, senza dover decodificare manualmente il file del certificato, è il comando

```
openssl x509 -in certificato.pem -text -noout
```

Se diamo una occhiata a un certificato valido, otterremo questi dati:

```
Common Name: RapidSSL CA
Organization: GeoTrust, Inc.
Country: US
Valid From: February 19, 2010
Valid To: February 18, 2020
Issuer: GeoTrust Global CA, GeoTrust Inc. Write
  review of GeoTrust
```

Invece, il file malevolo (che si può scaricare, per fare dei test, dall'indirizzo ***http://bit.ly/lm191hackingzone***) restituirà un errore. Se, infatti, il file non viene codificato correttamente è impossibile recuperare i vari parametri. È anche impossibile recuperare una corretta chiave crittografica, ma di quella ce ne si accorgerebbe comunque in un secondo momento: il primo problema che si presenta è proprio l'impossibilità di risalire alla CA che ha emesso il certificato, per poterlo verificare. Se fate il test con OpenSSL, noterete che si limita a rispondere che il certificato non è valido o e danneggiato. In GNUtls, invece, una situazione di questo tipo causa il crash della libreria.

Quindi finché il certificato è autentico va tutto bene, il problema si pone solo nel caso in cui un server o un client vogliano causare un Denial of Service dall'altra parte e inviino un certificato appositamente falsato. Una situazione non tanto assurda: un attaccante che desidera disattivare un server web potrebbe connettersi inviando un certificato contraffatto, e causare il crash del server, che a quel punto non potrebbe più rispondere nemmeno agli altri utenti. Chiaramente, gli amministratori del server non impiegherebbero molto tempo a riavviarlo, ma con una adeguata botnet sarebbe possibile continuare a mandare in crash il server con poco sforzo. In realtà, GNUtls controllava già i parametri forniti dal certificato, ma la funzione era stata scritta male. Invece di

```
ret = _gnutls_x509_read_value(cert->cert,
  "tbsCertificate.si
```

era stato scritto

```
ret = _gnutls_x509_read_value(cert->cert,
  "signatureAlgorithm.parameters", &sp2);
```

Si è trattato di un semplice errore di digitazione: chi ha inserito questa funzione ha copiato il codice da un'altra parte e si è dimenticato di aggiustare il nome del parametro. Un problema più comune di quanto si vorrebbe pensare.

Fig. 2 • La patch aggiunge solo due righe di codice, svuotando la variabile incriminata del contenuto

LA SOLUZIONE

Per fortuna, la soluzione è stata implementata quasi immediatamente. Il ricercatore del Google Project Zero ha infatti proposto un semplice bugfix che è stato subito accettato dagli autori di GNUtls e integrato nel codice sorgente della libreria. Aggiungendo due sole righe di codice alla funzione incriminata:

```
cleanup:
        gnutls_free(signature->data);
        signature->data = NULL;
        signature->size = 0;
        return result;
```

i dati vengono eliminati, e non si corre il rischio di un accesso dopo la liberazione del puntatore.

La nuova versione di GNUtls, che include questo bugfix, è già disponibile e, al momento in cui scriviamo, sta per essere inserita nei repository delle principali distro GNU/Linux.

La libreria alternativa, OpenSSL, non ha questa vulnerabilità, ma ovviamente non tutti possono rivolgersi ad essa. Questo perché solo GNUtls è davvero compatibile con la licenza GNU GPL, quindi i programmi rilasciati sotto la GNU GPL non possono usare OpenSSL senza inserire una apposita eccezione nella propria licenza.

NETPLAN: COME USARLO E COME RIMUOVERLO

Netplan nasce per semplificare la configurazione della rete di un server, soprattutto per chi deve gestire grandi pool di server contemporaneamente, ma non tutti lo apprezzano

Da ormai più di due anni Ubuntu ha introdotto Netplan, un livello di astrazione per la configurazione della rete. In effetti esistono diversi meccanismi per configurare la rete, e non è raro trovarsi a dover gestire dei server che usano strumenti diversi. Magari su alcuni server bisogna usare NetworkManager, magari su altri si ricorre a Networkd. Finché si controllano solo un paio di server si può fare tutto a mano. Ma se i numeri salgono, la cosa comincia a essere complicata. Per questo motivo Canonical ha pensato di sviluppare un livello di astrazione: un renderer che utilizza una sintassi standard valida per ogni sistema, e poi provvede automaticamente a tradurre la propria sintassi in un file di configurazione adatto per il sistema supportato da ciascun server. Netplan non è quindi un gestore della rete: è solo uno strumento che permette di configurare tutti i server con lo stesso linguaggio, appoggiandosi ai principali gestori della rete già esistenti. L'idea non è sbagliata, anche se il classico poco preavviso di Canonical ha fatto storcere il naso a molti.

CONFIGURARE LA RETE CON NETPLAN

La configurazione della rete via NetPlan si può fare con dei file in formato YAML, creando un file nella cartella **/etc/netplan** oppure modificando uno dei file esistenti (per esempio **01-network-manager-all.yaml**). Il formato tipico è il seguente:

```
network:
   Version: 2
   Renderer: NetworkManager/ networkd
   ethernets:
      DEVICE_NAME:
         Dhcp4: yes/no
         Addresses: [IP_ADDRESS/
                          NETMASK]
         Gateway: GATEWAY
         Nameservers:
            Addresses:
         [NAMESERVER_1, NAMESERVER_2]
```

Naturalmente, se si abilita il DHCP non è necessario indicare la configurazione IP. Basta quindi scegliere se appoggiarsi a NetworkManager oppure a Networkd, e se configurare manualmente un IP statico. Dopo aver scritto il file, si può provare la nuova configurazione col comando

```
netplan try
```

Se tutto funziona correttamente, si può abilitare definitivamente la configurazione:

```
netplan apply
```

In caso di errori, si può aggiungere l'opzione **-d** per avere informazioni di debug. Per sicurezza, bisogna riavviare il gestore a cui si è fatto riferimento:

```
systemctl restart network-manager
systemctl restart system-networkd
```

Il corrispettivo del vecchio **ifconfig** è il comando

```
ip a
```

In questo modo si può verificare che la configurazione sia cambiata. Nella documentazione ufficiale sono presenti molti esempi pronti all'uso (***http://bit.ly/netplanesempi***).

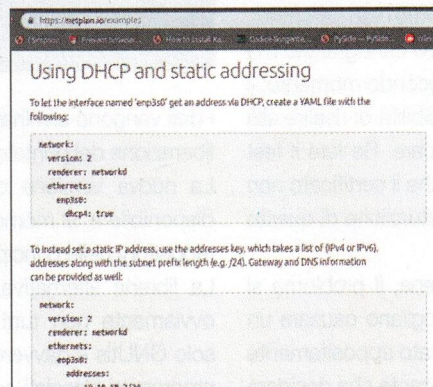



Fig. 1 • Gli esempi sul sito netplan.io

RIMOVERE NETPLAN

Se NetPlan non ci convince, e vogliamo farne a meno per continuare a gestire la rete come abbiamo sempre fatto, possiamo rinunciarvi. Innanzitutto, è possibile fare l'optout al momento dell'installazione aggiungendo

```
netcfg/do_not_use_netplan=true
```

nella riga di boot del sistema che viene usato per installare Ubuntu (es: un DVD live). Per disabilitare NetPlan su un sistema in cui è già installato, bisogna prima di tutto installare **ifupdown**:

```
apt-get install ifupdown
```

È poi necessario configurare **/etc/network/interfaces** come si è sempre fatto. Si deve anche specificare manualmente il server DNS che si vuole usare nel file **/etc/systemd/resolved.conf**:

```
DNS=8.8.8.8 8.8.4.4
```

E finalmente abilitare la configurazione:

```
ifdown --force enp0s3 lo && ifup -a
systemctl unmask networking
systemctl enable networking
systemctl restart networking
systemctl stop systemd-networkd.socket
     systemd-networkd networkd-dispatcher
              systemd-networkd-wait-online
systemctl disable systemd-networkd.
     socket systemd-networkd networkd-
   dispatcher systemd-networkd-wait-online
systemctl mask systemd-networkd.socket
     systemd-networkd networkd-dispatcher
              systemd-networkd-wait-online
apt-get --assume-yes purge nplan
                              netplan.io
systemctl restart systemd-resolved
```

A questo punto NetPlan dovrebbe essere completamente disabilitato.

Un Enigma da risolvere

Da sempre gli eserciti hanno cercato di segretare le proprie comunicazioni e intercettare quelle degli altri, ma oggi è un po' più complicato capire chi sia il "nemico"

La storia dell'uomo è, sotto molti aspetti, la storia delle guerre che si sono succedute. E la storia delle guerre che si sono succedute è, spesso, la storia dell'intelligence. Persino nell'antichità battaglie e guerre sono state vinte anche da piccoli eserciti contro grandi eserciti grazie a segreti scambi di informazioni. Segreti perché, tipicamente, bisogna far passare informazioni dal territorio del nemico al proprio, e di solito al nemico questa cosa non piace. Nell'antichità ci sono testimonianze di un meccanismo per nascondere i segreti piuttosto singolare: rasare la testa di una persona, scrivere il messaggio sul cuoio capelluto, e aspettare che i capelli ricrescano. Poi si inviava la persona oltre la frontiera senza che nessuno potesse sospettare nulla. E il destinatario doveva solo radere i capelli per leggere il testo. Naturalmente era necessario che il messaggero non si lavasse i capelli, ma questo non era un problema nell'antichità perché tanto i capelli non se li lavava comunque nessuno.

DA ROMA ALLA GERMANIA

Dopo un po' di tempo vennero inventati i parrucchieri, e la gente cominciò a lavarsi e tagliarsi spesso i capelli. A quel punto divenne necessario inventare un altro modo per nascondere i messaggi: la crittografia. Il problema della crittografia è che in linea di massima richiede l'uso di logica e matematica. E sono due cose che la maggioranza della popolazione non ha mai apprezzato. Per questo motivo si è sempre cercato di costruire dispositivi che rendessero cifratura e decifratura dei messaggi molto semplici. **Cesare**, per esempio, utilizzava due dischi concentrici per far ruotare le lettere e creare un nuovo alfabeto con cui scrivere e leggere i messaggi. Praticamente una roulette per crittografi: se punti sul numero giusto di rotazioni vinci il potere di decifrare i messaggi segreti. Pare che funzionasse molto bene, perché i suoi avversari erano troppo impegnati a trovare un posto ancora libero sulla sua schiena per piantare un coltello per riuscire a capire come leggere i messaggi.

Fig. 1 • Il cifrario di Cesare

Nel corso dei secoli sono nati molti altri sistemi per cifrare messaggi, e ovviamente anche dispositivi meccanici per forzare la cifratura dei messaggi: quando c'è qualcuno che vuole nascondere qualcosa, esiste anche qualcuno che vuole scoprire quel segreto. Agli inizi del '900 è arrivata l'elettronica, con la possibilità di realizzare combinazioni molto complicate in spazi tutto sommato abbastanza ristretti, e senza troppi problemi da polvere e urti. Naturalmente, l'elettronica veniva utilizzata già dall'800 per trasmettere messaggi: il telegrafo, il telefono, e la radio sono comparsi nel diciannovesimo secolo, per soddisfare il crescente bisogno della popolazione di spettegolare sugli affari degli altri. Questi sistemi, però, non permettevano una facile crittografia delle comunicazioni, se non con metodi tanto semplici da essere troppo facili da forzare. Negli anni'20 la situazione cambia grazie a **Enigma**, la macchina crittografica più famosa. Inventata da un ingegnere tedesco, utilizzava dei rulli e una serie di spinotti per collegare le varie lettere, implementando l'algoritmo di cifratura tramite il circuito che si veniva a creare. La macchina divenne famosa soprattutto perché utilizzata dall'esercito tedesco durante la seconda guerra mondiale.

UNA VERA BOMBA

Gli appassionati di computer sanno che Enigma venne forzata grazie al primo calcolatore elettromeccanico: la **Bomba** del polacco Marian Rejewski. Si trattava però di un sistema molto semplice e non programmabile, quindi appena i tedeschi iniziarono a usare una versione modificata di Enigma per scopi militari la Bomba non funzionò più. Alan Turing riuscì a trasformarla in un ingombrante e delicato calcolatore programmabile, ottenendo il grande vantaggio di poter modificare il funzionamento della macchina senza bisogno di ricostruirla da capo, e iniziando la grande tradizione di dare un pugno ai calcolatori che si bloccano.

Naturalmente, Enigma era complicata, e il brute force eseguito dalle Bombe non permetteva davvero di decifrare il messaggio: permetteva solo di restringere il campo a una manciata di combinazioni possibili, da provare a mano su una replica di Enigma per trovare la corretta chiave crittografica. Un grande risultato, comunque, anche se c'era un problema di lentezza: era necessario troppo tempo perché le Bombe finissero il lavoro, e soprattutto agli inizi si riuscivano a decifrare i messaggi troppo tardi perché potessero essere utilizzati davvero. E sapere che i tedeschi avevano l'intenzione di affondare una corazzata britannia ore dopo che era già successo serviva a poco.

Un collega di Turing, chiamato Gordon Welchman, ebbe una idea per velocizzare tutto il processo: lavorare sulle abitudini. Per esempio, i tedeschi avevano l'abitudine di iniziare alcuni messaggi con il saluto al cancelliere, e a un certo orario venivano sempre inviati bollettini metereologici, quindi si potevano dedurre le prime parole di

questi messaggi. Utilizzando queste parole come suggerimento per l'algoritmo delle Bombe diventava possibile rintracciare la chiave crittografica molto più rapidamente. Praticamente, invece di un puro brute force veniva fatto un attacco basato su un dizionario. La stessa tecnica che ancora oggi da grandi frutti con le password di Windows.

I METADATI VALGONO PIÙ DEI DATI

Dopo avere scoperto che la conoscenza di parole chiave nel testo velocizzava davvero il funzionamento della Bombe, Welchman decise di inventare quella che oggi chiamiamo **traffic analisys**. In poche parole, cominciò a leggere tutti i messaggi intercettati e decifrati ogni giorno, per notare dei pattern ricorrenti da parte di alcuni operatori. Scoprì che un agente tedesco su suolo britannico inviava un messaggio ogni volta che un aereoplano partiva da una pista di volo britannica. E che quel messaggio, molto breve, era scritto sempre con la stessa sintassi. La tipica precisione tedesca. Quindi, quando non si riusciva a scoprire la chiave crittografica dai normali messaggi, bastava dare l'ordine di far decollare, anche senza altri motivi, un aereo da quella stessa pista di volo e nel giro di pochi minuti si poteva intercettare un messaggio molto facile da decifrare. Dando quel messaggio e la sua ipotetica ricostruzione alla bomba si poteva in poche ore ottenere la chiave crittografica che i tedeschi avrebbero utilizzato per tutto il resto della giornata.

L'attenzione di Welchman si spostò poi verso i **metadati**. Analizzando i testi si accorse infatti che osservando mittenti e destinatari era possibile creare una lista dettagliata dei rapporti all'interno dell'esercito tedesco. E si accorse anche che queste informazioni erano spesso molto più interessanti del contenuto stesso dei messaggi. Era infatti possibile decifrare messaggi molto banali, come saluti, auguri, quasi pettegolezzi, e comunicazioni personali per le famiglie dei soldati. Ma ciascuno di essi permetteva di ricostruire una mappa di quali compagnie dell'esercito tedesco fossero in contatto tra loro. Si poteva capire quanto grande fosse ciascun accampamento, e intuire persino quanto fossero distanti tra loro.

Fig. 2 • Gordon Welchman ha inventato la traffic analisys durante la Seconda Guerra Mondiale

UNA VERITÀ SCOMODA

Negli anni '80 Welchman pubblicò la sua storia in un libro, che venne ostacolato dal governo degli Stati Uniti. In una intervista commentò: "mi sembra che alcune di queste informazioni siano state tenute segrete per troppo tempo: si fanno più danni ingannando i propri cittadini sulla storia della seconda guerra mondiale piuttosto che dicendo la verità su come è andata". La realtà è che gli americani consideravano pericolosa la rivelazione delle attività di Welchman perché stavano usando le sue tecniche di traffic analysis per spiare i sovietici. A decenni di distanza, la preoccupazione di Welchman si è concretizzata, considerando l'analisi dei metadati da parte dell'**NSA** rivelata da Snowden. Abbiamo scoperto che queste tecniche, nate con la sola intenzione di scoprire in anticipo le mosse dei criminali di guerra, sono oggi usate estensivamente contro tutti noi, violando non soltanto la privacy ma anche la presunzione di innocenza, visto che ciascuno di noi viene costantemente sorvegliato preventivamente. Il comico John Oliver interpretò la cosa come una minaccia alla libertà di inviare la foto del proprio pene a un'altra persona senza che la stessa foto venga vista da decine di analisti dell'NSA. Pare che oggi lo stratagemma di radersi i capelli, scrivere sul cranio nudo, e aspettare la ricrescita sia l'unico modo rimasto per trasmettere, senza essere intercettati, testi e immagini. E questo include le dick pics. Il che, a pensarci bene, sembra un'ottima forma di protesta contro la sorveglianza governativa totale.

Fig. 3 • Edvard Snowden ha rivelato nel 2013 quanto sia diffusa l'analisi dei metadati da parte dell'NSA

Billy, the sysadmin cat